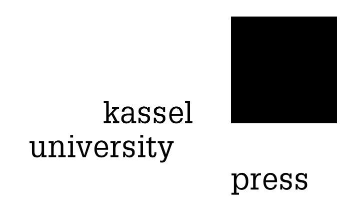


Anwendung der EDV im Arbeitsschutz

Lehrbuch und Nachschlagewerk für Studenten der Sicherheitstechnik
und für Fachkräfte der Arbeitssicherheit

Uwe Juergen Franke

Die Deutsche Bibliothek - CIP-Einheitsaufnahme
Franke, Uwe Juergen
Anwendung der EDV im Arbeitsschutz : Lehrbuch und Nachschlagewerk für Studenten der Sicherheitstechnik und für Fachkräfte der Arbeitssicherheit / Uwe Juergen Franke. - Kassel : kassel univ. press, 2001. - X, 276 S. : Ill.

ISBN 3-933146-29-1

Umschlaggestaltung: 5 Büro für Gestaltung, Kassel
Druck und Verarbeitung: Zentraldruckerei der Universität Gesamthochschule Kassel
Printed in Germany

Vorwort

Wie verschiedene Erfahrungsberichte und Untersuchungen zeigen, hat sich der Einsatz von EDV auch im weiten Feld des Arbeitsschutzes und der Betriebs-/ und Anlagensicherheit als nützlich erwiesen und daher durchgesetzt. Um dieser Gegebenheit Rechnung zu tragen und um die Studenten mit den vielfältigen, auf dem Markt angebotenen Problemlösungen etwas vertraut zu machen, wurde an der Bergischen Universität Gesamthochschule Wuppertal die Vorlesung \`Anwendung der EDV in der Sicherheitstechnik´ angeboten. Die Autoren (Dr.-Ing. Ulrich Mattke und Dr. Uwe Franke), die diese Vorlesung aufgebaut hatten, befassen sich schon lange mit diesem Thema und gehen davon aus, dass das hierbei zusammengetragene Wissen für Studenten und Praktiker von Interesse sein könnte. Das Buch ist zum einen als Lehrbuch und als Informationsquelle für Studenten gedacht, die sich für eine Tätigkeit als Fachkraft für Arbeitssicherheit interessieren und zum anderen als Nachschlagewerk für in der Praxis stehende Fachkräfte für Arbeitssicherheit gedacht. Aufgrund der Nachschlagefunktion wurde sich bemüht, die Kapitel derart zu schreiben, dass jedes Kapitel für sich genutzt werden kann. Es werden bewusst einige Dinge weg gelassen, die bei einem Nachschlagewerk mit in den Anhang gehören, z.B. die UVVen zu Bildschirmarbeitsplätzen und die Gefahrstoffverordnung, um den Inhalt des Buches nicht ins uferlose geraten zu lassen.

Unser Dank gilt allen, die uns Infomaterial und andere Unterlagen zur Gestaltung des Buches überlassen haben.

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

1 Einführung

Böse Zungen sagen, “das Kennzeichen der Menschen sei die Faulheit. Er strebe immer danach, so wenig wie möglich tun zu müssen. Unter diesem Gesichtspunkt müsse die technische Entwicklung gesehen werden.”
Ob diese Sicht der technischen Entwicklung die Richtige ist, soll hier nicht erörtert werden und kann wohl auch nicht pauschal beantwortet werden. Auf jeden Fall ist auch in der Sicherheitstechnik das Bestreben vorhanden, die gegebenen Aufgaben so rationell und effektiv wie möglich zu erledigen. Eines der angewendeten Mittel, das sich auch in anderen Bereichen in großem Maße bewährt hat, ist die elektronische Datenverarbeitung, kurz EDV.

1.1 Das Hilfsmittel EDV und seine sicherheitstechnische Anwendung

Der Bereich der EDV-Anwendungen hat sich mit steigender Rechnerleistung immer weiter vergrößert. Die Anwendung der EDV beginnt beim \`einfachen´ Taschenrechner mit der Addition von Zahlen über elektronische Wörterbücher bis hin zur Simulation großtechnischer Anlagen und natürlicher Abläufe.
Bild 1-1 zeigt einen beispielhaften Überblick über verschiedene Aufgabenfelder, die mit dem Hilfsmittel EDV bearbeitet werden können.

Allgemeine Aufgaben der elektronischen Datenverarbeitung (EDV):	Datenaufnahme Datenspeicherung Datenverwaltung Datenverwertung Datenausgabe

Beispiele aus speziellen Gebieten:

Verwaltung/Vertrieb:	Textverarbeitung, Datenbanken, Statistikprogramme
Produktionstechnik:	CNC-Steuerungen, Robotersteuerungen, CAQ-Systeme
Konstruktion:	CAD-Systeme, Simulationssysteme
Forschung/Entwicklung:	Rechenprogramme, Simulationssysteme, Datenbanken
Arbeitsvorbereitung:	CNC-Steuerungen, Simulationssysteme, PPS-Systeme

Bild 1-1 Einsatzbereiche der elektronischen Datenverarbeitung

Viele der hier gezeigten Möglichkeiten werden in der Sicherheitstechnik angewendet. Im Bereich der Verkehrssicherheit wird sehr viel mit dem Mittel der Simulation gearbeitet, dazu kommen computergesteuerte Kontrollsysteme in Kraftfahrzeugen zu Lande, Wasser und Luft. Auch im Bereich Produktion wird die Simulation - natürlich in erster Linie nicht unter sicherheitstechnischen Gesichtspunkten - angewendet. In der Hauptsache werden verwendet insbesondere CNC-Steuerungen, Roboter-Steuerungen (i.d.R. auf Basis speicherprogrammierbarer Steuerungen [SPS]), Produktionsplanungssysteme (PPS) und Datenbanken.
In der (sicherheitsgerechten) Konstruktion liegt der Schwerpunkt des EDV-Einsatzes auf der Verwendung von CAD (Computer Aided Design) -Systemen. Hinzu kommen auch hier Datenbanken, speziell in der Form elektronisch gespeicherter Normteil-Bibliotheken. Datenbanken und Simulation sind im Bereich des Umweltschutzes die wichtigsten EDV-Hilfsmittel, ebenso im Bereich Reaktorsicherheit und Strahlenschutz.
In diesem Buch wird sich im wesentlichen auf die EDV-Anwendungsmöglichkeiten beschränkt, die für die praktische Arbeit einer Arbeitsschutzabteilung von Interesse sind. Herunter fallen zum Beispiel Textverarbeitung, Datenbankfunktionen und statistische Funktionen.

1.2 Festlegung der Begriffe Arbeitschutz und Arbeitssicherheit

In diesem Buch wird sich auf das Arbeitsgebiet einer *Arbeitsschutz*-Abteilung bzw. einer Fachkraft für *Arbeitssicherheit* (FaSi) beschränkt. Um Missverständnissen vorzubeugen wird abgeklärt, was in diesem Buch unter den Begriffen *Arbeitsschutz* und *Arbeitssicherheit* verstanden wird.
Arbeitsschutz ist die Umsetzung der Sicherheitstechnik direkt am Arbeitsplatz. Darunter fallen alle technischen und organisatorischen Maßnahmen, um den Werktätigen vor den Gefahren (des) am Arbeitsplatz(es) bzw. der auszuübenden Tätigkeit zu schützen. Nach Samlowski spielt sich der Arbeitschutz "in einem kognitiven Präventionsregelkreis von Planung, antizipatorischer Analyse, Bewertung und modifizierter Planung ab. Je nach dem Grad der Bewusstheit möglicher negativer Effekte der Arbeit auf die Gesundheit ist jede Arbeit in diesem Sinne mehr oder minder zugleich Arbeitsschutz, wenngleich der professionell im Arbeitsschutz Tätige ein weit ausgefeilteres System von Wissen und Erfahrung über negative gesundheitliche Effekte, eben Risiken, und deren Vermeidung sein eigen nennen kann als der `nur´ Arbeitende." /Sam, S.48/
Die Sicherheitstechnik im allgemeinen Verständnis greift in der Regel auf sicherheitswissenschaftlich weiterentwickelte Methoden aus dem Ingenieurbereich zurück. Arbeitssicherheit umfasst den Arbeitsschutz, beinhaltet - bezogen auf den Betrieb - auch Arbeitsmedizin, sicherheitsgerechte Kon-

struktion, Ergonomie, Vermeidung (oder zumindest Schutz vor) gefährlicher (n) Stoffe, Brand und Explosionsschutz etc.

1.3 Aufgaben einer Fachkraft für Arbeitssicherheit (FaSi)

Um ein EDV-System beschaffen bzw. einführen zu können, muss im Vorfeld abgeklärt werden, welche Aufgaben mit diesem System durchgeführt werden sollen. Hier geht es darum, die Aufgaben einer FaSi zu erleichtern bzw. zu vereinfachen, zum Beispiel sogenannte Routinetätigkeiten automatisieren, Verwaltungstätigkeiten beschleunigen.
Prinzipiell kann der Aufgabenbereich einer FaSi mit den Stichworten:
“Unterstützung - Beratung - Untersuchung - Beobachtung - Einwirkung”
beschrieben werden. /Ste, S. 15/
Eine etwas genauere Aufgabenbeschreibung wird in Bild 1-2 gegeben.

Prinzipiell:	Den Unternehmer/die Geschäftleitung/den Behördenleiter in Belangen des Arbeitsschutzes unterstützen
dazu gehören:	Beratung in sicherheitstechnischen Fragen
	Sicherheitstechnisches Überprüfen
	Mitteilen festgestellter Mängel
	Unterbreiten von (Verbesserungs-) Vorschlägen
	Hinwirken auf sicherheitsgerechtes Verhalten
	Fördern des Sicherheitsbewusstseins
	Schulung und Betreuung z.B. der Sicherheitsbeauftragten
	Beobachten/Kontrolle der Schutzmaßnahmen
	Zusammenarbeit mit dem Betriebsrat/Personalrat
	Zusammenarbeit mit dem Betriebsarzt
	Zusammenarbeit mit den Aufsichtsdiensten
	Im Arbeitsschutzausschuss mitwirken

Bild 1-2 Aufgabenfeld einer Fachkraft für Arbeitssicherheit

Die Beschränkung auf die Angabe solcher relativ allgemeiner Stichworte ist für eine Aufgabenbeschreibung eines einzuführenden EDV-Systems eine ungenügende Grundlage. Hierzu sind detailliertere Betrachtungen notwendig wie sie z.B. von Grassl/Sinks - Arbeitsschutz im öffentlichen Dienst - bezüglich des Tätigkeitsbereiches einer FaSi durchgeführt wurden. Deren Ergebnisse sind in Tabelle 6-1 (findet sich im Anhang) zusammengefasst. Ähnliche Resultate bietet auch die neuere Untersuchung von Michael Scheil /Sche1 und Sche2/, die auf den Ergebnissen einer vom Fachgebiet Sicherheitstechnik/Produktion der Bergischen Universität Gesamthochschule Wuppertal in den Jahren 1994/95 durchgeführten Befragung beruht. Was Scheil besonders betont, sind die vielfältigen Beauftragtenfunktionen, welche die FaSi oft noch inne hat. Darunter fallen z.B. Umweltschutz in allen seinen Schattierungen, Brand- und Explosionsschutz, Qualitätssicherung, Materialwirtschaft und auch in manchen Fällen der Datenschutz. /Sche2, S. 295/

1.4 Einsatzgebiete der EDV im Arbeitsfeld einer FaSi

Einige Aufgaben einer FaSi können mittels EDV-Unterstützung durchgeführt und dadurch vereinfacht und erleichtert werden.
Mit dem Hilfsmittel Textverarbeitung kann der Schriftverkehr rationalisiert werden, der bei der sicherheitstechnischen Beratung von Vorgesetzten, Unternehmern, Behördenleitern etc. anfällt.
Für die Überprüfung von Grundstücken, Gebäuden, anderen baulichen Anlagen sowie technischer Anlagen kann ein sogenannter elektronischer Kalender und eine z.B. in einem Textverarbeitungsprogramm erfasste und gespeicherte Checkliste eine Hilfe sein.
Ein Textverarbeitungsprogramm ist auch sinnvoll als Hilfsmittel beim Mitteilen der beim Beobachten festgestellten Mängel. Das Vorschlagen von Maßnahmen zur Beseitigung der festgestellten Mängel kann ebenfalls mittels eines innerhalb einer Textverarbeitung gespeicherten Formblattes effizienter gestaltet werden.
Die Erstellung von Arbeitsanweisungen, Richtlinien und Merkblättern (z.b. für den Umgang mit Gefahrstoffen) kann mit Hilfe einer Datenbank sowie eines Textverarbeitungsprogramms deutlich erleichtert werden.
Auch bei der Gestaltung und Bewertung von Arbeitsverfahren unter Berücksichtigung der Punkte: Arbeitsabläufe, Arbeitsmittel, Gestaltung und Aufbau der Arbeitsplätze oder Arbeitsbereiche sowie der Arbeitsumgebung bieten sich Datenbanken als Hilfsmittel an. EDV-gestützte Arbeitsplan- und Ablaufplanerstellung sind in diesem Aufgabenfeld schon länger aus fertigungstechnischer und ökonomischer Sicht in Anwendung.
Die Einführung, Änderung und Verwaltung der `Persönlichen Schutzausrüstung´ kann gleichfalls mittels einer Datenbank und einer Textverarbeitung vereinfacht werden.

Weitere Aufgaben wie Schulung und Betreuung der Sicherheitsbeauftragten, die Zusammenarbeit mit dem Betriebs-/Personalrat, dem Betriebsarzt, außerbetrieblichen Stellen des Arbeitsschutzes usw. können ebenso durch den Einsatz einer Textverarbeitung bezüglich des Schriftverkehrs unterstützt werden. Die eigentlichen Kontroll- bzw. Überwachungsaufgaben können derzeit (1999) nur unter sehr großem finanziellen und technischen Aufwand mittels Computersysteme vereinfacht oder gar automatisiert durchgeführt werden.
Je nach anfallender Menge der Schadensmeldungen, der Beinahe-Unfälle und der Unfälle wird bei der Aufnahme und Speicherung der hierbei anfallenden Daten eine Datenbank von Nutzen sein. Für die Auswertung dieser Daten kann ein Statistikprogramm eine wesentliche Unterstützung darstellen. Der notwendige Schriftverkehr wegen dieser Ereignisse mit z.B. der Geschäfts-/Behördenleitung sowie dem Unfallversicherungsträger (bei Anfallen von meldepflichtigen Arbeitsunfällen) kann mit Hilfe einer Textverarbeitung ebenso rationalisiert werden.
Dieser letztgenannte Aufgabenbereich `Unfalldatenerfassung und -bearbeitung´ war der Ausgangspunkt für die Entwicklung eigenständiger Software, welche die Arbeit der FaSi erleichtern soll.

1.5 Entwicklungsgeschichte der rechnergestützten Arbeitssicherheit

Die Anwendung der EDV im Arbeitsschutz begann sich Mitte der achtziger Jahre immer stärker durchzusetzen. Dokumentiert liegt dies vor für das System der `Rechnergestützten Arbeitssicherheit (RASI)´ der Hoesch AG. Die Entwicklung und Einführung als auch die Gründe der Entwicklung sowie die Hintergründe zur Entwicklung von `RASI´ werden im 1986 erschienenen Projektbericht von W. Hagen, A. Pauwels, W. Suttrop und O. Wichert beschrieben:
Die Unfallzahlen der Hoesch AG waren in den letzten 14 Jahren (von 1984 aus gesehen) auf die Hälfte gesunken. Es wurde bei Hoesch erkannt, dass es notwendig ist, ein verfeinertes Instrumentarium für genauere Analysen einzusetzen, wenn ein weiteres Absinken der Unfallzahlen erreicht werden soll. Es wurde weiterhin festgestellt, dass das "Gebiet der Unfallanalyse, der Unfallursachenermittlung und der Gefährdungsermittlung vom methodischen Ansatz und auch vom erforderlichen Zeitaufwand entwicklungs- und verbesserungsbedürftig ist."/Hag, S. 1/
Als eines der möglichen Mittel zur Verbesserung der Arbeitseffizienz wurde der Einsatz von Kleinrechnern (PCs) gesehen. Dazu war es aus Sicht der Autoren notwendig, spezifische - an die Belange des Arbeitsschutzes angepasste - Programme zu entwickeln. Diese Programme sollten u.a. die Sicherheitsfachkräfte "von zeitaufwendigen Unfallanalysen und -statistiken" entlasten.

"Ein kleiner Arbeitskreis erhielt den Auftrag, ein Konzept zu erarbeiten. Die beteiligten Vorstände der Hoesch AG und der Hoesch Hohenlimburg AG billigten das Konzept unter der Maßgabe zu prüfen, ob öffentliche Mittel in Anspruch genommen werden können. Diese Maßgabe führte zur Beantragung einer finanziellen Förderung beim Bundesminister für Arbeit und Sozialordnung, vertreten durch die Bundesanstalt für Arbeitsschutz in Dortmund. Nach der Bewilligung der Förderung konnte das Projekt zum 1. September 1984 begonnen werden." /Hag, S. 3/

Unter Berücksichtigung aller gesetzlichen Auflagen (Information und Beteiligung des Betriebsrats, Information der Arbeitsschutzausschüsse etc.) erfasste und untersuchte eine Projektgruppe die bisherigen Verfahrensweisen. Infolge der Ergebnisse dieser Betrachtungen wurde aufgrund des ermittelten Platz- und Rechenbedarfs ein IBM-PC/AT ausgewählt. Die Programme wurden in Cobol erstellt, da in dieser Programmiersprache die meiste Erfahrung gegeben war.

Auf der A + A -Veranstaltung (Messe und Kongress) in Nürnberg 1986 wurde zu diesem Thema erstmalig eine Sonderausstellung durchgeführt. Vierzehn verschiedene Anbieter präsentierten Programme für verschiedene Einsatzgebiete des Arbeitsschutzes. Angeboten wurden Programme zur Anlagenüberwachung, zur Ausbildungsplanung, zum Brandschutz, zur Instandhaltung, zum Umweltschutz, zur Unfalldatenerfassung und Unfall-Datenverarbeitung. Laut der Fachzeitschrift `Sicher ist Sicher´ war das Interesse groß. Trotz der vorhandenen Euphorie schrieben sie jedoch: "Es war jedoch nicht alles Gold, was da glänzte." /SiS 2/87, S. 82/ Die Programme wiesen noch deutliche Mängel auf bezüglich der Arbeitsinhalte, der Softwareergonomie und des Datenschutzes. Aus unserer Sicht beurteilte Schubert im Jahre 1991 die Ausstellung von 1986 zu hart: "Es herrschte damals kein größeres Gedränge an den dortigen Ständen. Aus heutiger Sicht rechtfertigten die angebotenen Programme auch kaum ein größeres Interesse." /Schu, S. 1/

Auf der zweiten Sonderschau in Hannover 1988 waren zwölf Anbieter für die Sonderschau angemeldet. Einige andere Anbieter beteiligten sich nicht an der Sonderschau, sondern demonstrierten ihre Programme an den normalen Ausstellungsständen innerhalb der `gewöhnlichen´ Fachausstellung zum Thema Arbeitsschutz.

Die Zahl der Anbieter und Programme steigerte sich rasch. Schon im März 1991 gab Hartung in einer Marktübersicht 37 verschiedene Anbieter der von ihm als CAS-Programme bezeichneten Software an. Unter der Abkürzung CAS versteht Hartung den `Computerunterstützten Arbeitsschutz´ (engl.: Computer Aided Safety). /Har1/

Diese Programme zeichneten sich durch deutliche Verbesserungen in den oben kritisierten Punkten aus, waren selbstverständlich noch immer verbesserungsfähig.

In einer im Frühjahr 1995 durchgeführten Studienarbeit konnte Heidi Wunenburger /Wun/ ein weiteres deutliches Ansteigen der Zahl der angebotenen Programme im Bereich Arbeitssicherheit registrieren. Allein die Zahl der verschiedenen Gefahrstoffprogramme lag über vierzig. Und Frau Wunenburger betonte ausdrücklich, dass die Arbeit keinen Anspruch auf Vollständigkeit erhebt.
Auf den letzten Arbeitsschutzmessen waren die Anbieter von Arbeitsschutz-Software nicht in einer Sonderausstellung zusammengefasst. Die angebotenen Programme zeigten zum großen Teil sehr deutlich den Einfluss neuerer softwareergonomischer Erkenntnisse und waren oft von den neuen Softwareentwicklungen geprägt (Anpassung an Windows bzw. an die Windows-Oberfläche).
In der Regel ist die Software für die Aufgaben des Arbeitsschutzes für IBM-kompatible PCs programmiert. Als Betriebssystem wird DOS und bei den neuen Entwicklungen auch die Benutzeroberfläche Windows benötigt. In Ausnahmefällen sind auch einige Programme für Großrechner entwickelt worden. Dies gilt insbesondere für die Gefahrstoffdatenbanken, die behördlicherseits entwickelt und benutzt werden.

2. Hardware und Betriebssysteme

Das Arbeitsmittel Rechner kann man folgendermaßen klassifizieren:

- Großrechner,
- Rechner mittlerer Datenleistung,
- Workstations und
- Personal-Computer (PC)

Die Grenzen zwischen den einzelnen Rechnerklassen sind fließend und ändern sich durch den schnellen technischen Fortschritt dauernd. Daher soll auf diese Aufteilung und ihre Unterschiede nicht weiter eingegangen werden. Wie schon in der Einleitung erwähnt, wird sich in der Hauptsache am Aufbau eines PCs orientiert.

Rechner bestehen aus den Komponenten Hardware und Software. Software ist der geistige Inhalt eines Rechners, d.h. der Teil, der es ermöglicht, dass mit einem Rechner bestimmte Aufgaben erledigt werden können. Mit Hardware dagegen werden die Teile des Rechners bezeichnet, "die man mit den Händen im wahrsten Sinne des Wortes anfassen kann"./Dic, S. 21/

[Verwendet man ein umfassenderes Verständnis des Begriffs 'Hardware' werden auch die Arbeitsplatzgeräte wie Tisch und Stuhl etc. darunter gefasst.]

Prinzipiell gehört zur Hardware der eigentliche Rechner, wenigstens ein Eingabegerät und wenigstens ein Ausgabegerät.

2.1 Eingabegeräte

In Bild 2-1 werden die gängigsten Eingabegeräte aufgeführt:

	Eingabegeräte
Tastatur	*in der Regel mit 102 Tasten; auch sogenannte ‘Minitastaturen’ mit 81 Tasten*
Maus	*meistens mit 2 Tasten; Kabelverbindung*
Trackball	*erstattet die Maus beim Laptop*
Graphiktabletts	*werden mit ‘Lupe’ und/oder Tastenstift verwendet*
Scanner:	
• *Flachbettscanner*	*man arbeitet wie mit einem Kopierer*
• *Handscanner*	*werden manuell über die Vorlage gezogen*
Strichcodeleser	*als Tisch- und Handgeräte*
Magnetkartenleser	*(oder -schreiber)*

Bild 2-1 Eingabegeräte

Tastatur /vgl. Dic, S.67 ff./

Um Daten einzugeben wird am häufigsten die Tastatur (Keyboard) verwendet. Auch kann von der Tastatur aus das Betriebssystem und die Anwendersoftware gesteuert werden. Man sollte bei den Tastaturen auf eine ausreichende Qualität bezüglich Belastungsfähigkeit und Ergonomie achten. Eine gute Tastatur ist nicht in den PC integriert. Sie ist in vier Tastenblöcke eingeteilt:

"1. dem alphanumerischen Tastenblock mit Buchstaben, Ziffern, Sonder- und Steuerzeichen zur Eingabe von Daten, Texten und zur Programmsteuerung;

2. der Funktionstasteneinheit aus mindestens 12, besser noch 18 Tasten bestehend. Viele Programme nutzen die Funktionstasten zum Aufrufen von Befehlen und erlauben darüber hinaus das Belegen von zusätzlichen Funktionstasten;

3. dem separaten Cursorblock, der aus vier Pfeiltasten besteht und zum Steuern des Cursors auf dem Bildschirm bebraucht wird und

4. der Zehnertastatur, wie sie von Rechenmaschinen her bekannt sind, um Zahlenkolonnen einhändig eingeben zu können."/Dic/

In der DIN-Norm 2137, Teil 2 ist der Aufbau einer Tastatur festgelegt.

Grafiktableau (Digitalisiertablett) /vgl. Dic, S.67 ff./

Das Grafiktableau wird in der Regel nur im Bereich des technischen Zeichnens bzw. Konstruierens verwendet. EDV-gestützt spricht man dann von Computer-Aided-Design (CAD). Das Brett ist in zwei Bereiche aufgeteilt. Im größeren Bereich kann die Zeichnung erstellt werden. Der kleinere Bereich ist in Raster aufgeteilt (sogenannter Menübereich). In den einzelnen Rasterfeldern sind die Programmbefehle und Optionen abgedruckt. Diese können mit einer Fadenkreuzlupe oder dem Digitalisierstift angewählt werden. Die Anwendungsmöglichkeiten und -Bereiche sind stark vom verwendeten Softwarepaket abhängig. Der Gebrauch des Grafiktableaus ist rückläufig, da viele CAD-Programme die Menüs nun auf dem Bildschirm darstellen können.

Maus, Trackball /vgl. Imp, S. 198/

Die meisten PC-Programme sind für den Gebrauch mittels Maus oder Trackball eingerichtet. Bei vielen Programmen ist die Maus unverzichtbares Hilfsmittel. Je nach System haben die Mäuse eine (Apple), zwei (Microsoft) oder drei (Mouse-Systems) Tasten. Das Anwendungsprinzip ist grundsätzlich gleich; die Maus wird über einer Oberfläche bewegt bis das gewünschte Ziel (am Bildschirm sichtbar) erreicht ist. Durch Drücken einer oder zweier Tasten wird die gewünschte Funktion etc ausgelöst.

Der Trackball ist im Prinzip eine umgedrehte Maus. Er wird angewendet, wenn der Platz für eine Maus nicht vorhanden ist, z.B. bei Laptops (tragbare PCs).

Scanner /vgl. Imp, S. 199/

Scanner dienen dazu, gedruckte Vorlagen wie Texte, Photos oder Zeichnungen in den Rechner einzulesen. Gescannte Informationen werden z.B. in Textverarbeitungsprogramme integriert, können aber auch direkt ausgedruckt oder über Faxkarten ausgegeben werden. Gebräuchlich sind Flachbettscanner und Handscanner. Flachbettscanner sind i.d.R. einfacher anzuwenden und liefern bessere Ergebnisse. Handscanner sind in der Anschaffung kostengünstiger. Für die Anwendung der Scanner ist ein entsprechendes Softwarepaket wichtig; normale Graphikprogramme sind nicht immer dazu ausgelegt, solche Daten aufzubereiten.

sonstige /vgl. Imp, S. 199/

Weitere Dateneingabegeräte sind Strichcodeleser und Magnetkartenleser. Strichcodeleser finden ihre Anwendung in der Warenwirtschaft, Magnetkartenleser in der Geldwirtschaft und im Verwaltungsbereich. Sie dienen dazu, relativ geringe Datenmengen einfach und schnell zur direkten Weiterverarbeitung in den Rechner einzugeben. Magnetkartenleser werden in vielen Fällen durch Chipkarten ersetzt.

2.2 Ausgabegeräte

Zur Datenausgabe werden verschiedene Arbeitsmittel verwendet. Die gebräuchlichsten sind Bildschirm und Drucker. In Bild 2-2 ist das Wesentliche zu Bildschirmen zusammengefasst.

Ausgabegeräte: Bildschirme (Monitore)	
LCD-Monitor	gewöhnlich mit Auflösung 640x480; VGA-kompatibel; häufig in Laptops
Monochrom-Monitore	in verschiedenen Größen (in Zoll angegeben), für Textverarbeitung gut geeignet
Farbmonitore	in verschiedenen Größen (in Zoll angegeben), in unterschiedlicher Auflösung (häufig 1024 x 768); besonders gut sind Farb-multisync-Monitore mit Trinitron Bildröhren

Bild 2-2 Ausgabegeräte - Bildschirme

Bildschirm /vgl. Dic, S.60 f./

Der Bildschirm ist neben der Tastatur das Hauptarbeitsmittel am Rechner. Die Dateneingabe wird am Bildschirm kontrolliert, (gerechnete) Ergebnisse können über den Bildschirm eingesehen werden.

Es wird unterschieden zwischen monochromen (einfarbigen) und farbigen Bildschirmen. Wesentlichen Einfluss auf die Arbeitsqualität mit Bildschirmen hat ihre Größe. Standard ist 1999 eine Größe von 15 oder 17 Zoll Diagonalgröße. Die Auflösung beträgt in der Regel 1024 x 768 Pixel. Für Graphik, CAD oder DTP-Anwendungen sollten größere Bildschirme mit besserer Auflösung verwendet werden; als eine gute Größe gelten 19 oder 21 Zoll große Bildschirme. Die Auflösung sollte mindestens 1640 x 1280 Pixel betragen. Es gibt digitale und analoge Schirme sowie Schirme mit fester als auch Schirme mit variabler Synchronisation. Die üblichen Schirme verwenden eine Kathodenstrahlröhre für den Bildschirmaufbau (Prinzip eines Fernsehers). In Ausnahmefällen (z.B. bei Laptops) verwendet man Plasma-Displays oder Flüssigkeitskristalle, um damit extrem flache Bildschirme bauen zu können. Qualitätsmerkmale der Schirme sind Auflösung und Bildwiederholfrequenz (vgl. Kpt. Ergonomie). Um vom Rechner aus einen Bildschirm steuern zu können, muss der Rechner über eine Graphikkarte verfügen.

Monochrome Bildschirme sind in der Regel 'Schwarz-Weiß-Schirme'. Sie werden für reine Textverarbeitung empfohlen. Sie werden jedoch kaum noch gebaut; d.h. sie sind schwer lieferbar. Farbmonitore sind preislich viel günstiger geworden und haben monochrome Bildschirme als Standard verdrängt. Dazu kommt, dass viele Betriebssysteme und auch andere Software auf Information durch Farbe setzen.

Bildschirme konnten im sogenannten Textmodus oder im Graphikmodus angesteuert werden. Im Textmodus können nur die 256 ASCII-Zeichen verarbeitet werden. Es lassen sich 25 Zeilen mit je 80 Zeichen darstellen. Dagegen wird im Graphikmodus jeder einzelne Bildpunkt für sich angesteuert. Jeder einzelne Pixel (Bildpunkt) kann gesetzt, gelöscht und farblich verändert werden. Der Grafikmodus ermöglicht die 'what you see is what you get' (WYSIWYG) -Darstellung; d.h. das was auf dem Bildschirm zu sehen ist wird so auch auf dem Ausdruck erscheinen. Diese Art der Darstellung erfordert jedoch schnelle und leistungsstarke Rechner (im Verhältnis zu Rechnern mit einem 286er Prozessor - vgl. Kpt. 2.3) und ist inzwischen Standard (Wer hat noch einen 286er PC?).

Lautsprecher

Eine (bisher) untergeordnete Rolle bei der (Daten-)Ausgabe spielt der Lautsprecher (Ausnahme Musikerstellung). In der Regel wird der Lautsprecher nur verwendet, um ungeplante Betriebszustände anzuzeigen, Warnungen zu verdeutlichen oder um auf Fehlermeldungen aufmerksam zu machen.

Drucker /vgl. Dic, S.72 ff./
Das neben dem Bildschirm wichtigste Ausgabegerät ist der Drucker. Man kann unterscheiden zwischen Druckern, die das Schriftzeichen als Ganzes auf dem Schriftträger haben und den Druckern, die das Zeichen aus Einzelpunkten zusammensetzen.
Eine weitere Möglichkeit der Unterscheidung ist die Gliederung in berührungslose (Non-Impact) und Anschlag- (Impact) Drucker, die in Bild 2-3 dargestellt ist.

Drucker		
Impact		Non-Impact
	Nadelmatrix	
Ganzzeichen		Punktmatrix
Typenrad		Laser
Kugelkopf		Tintenstrahl
Typenkorb		Thermotransfer

Bild 2-3 Ausgabegeräte - Drucker /nach Dic/

Typenraddrucker zeichnen sich durch ein gestochen scharfes Schriftbild aus. Durchschläge können erstellt werden. Der Buchstabe ist als ganzes vorhanden (entspricht elektrischer Schreibmaschine). Nachteilig sind die langsame Druckgeschwindigkeit (jeder Buchstabe muss für sich angefahren werden) sowie die Geräuschentwicklung. Da diese Drucker nicht graphikfähig sind, worden sie vom Markt genommen.
Nadeldrucker haben je nach Nadelanzahl ein deutlich schlechteres Schriftbild. Unterster Level sind 9 Nadeln, angeboten werden noch 18, 24 und 48 Nadeln. Auch Nadeldrucker sind recht laut und im 'Schönschreibmodus' (Near Letter Quality - NLQ) relativ langsam im Vergleich zum z.B. Laserdrucker. Sie sind preisgünstig (gewesen). Sie können jedes beliebige Zeichen drucken, bzw. auch für Graphiken verwendet werden, da die Zeichen aus Einzelpunkte zusammengesetzt werden. Als Papier kann Endlospapier als auch normales Schreibpapier verwendet werden. Nadeldrucker werden im Handel kaum noch angeboten, da Tintenstrahldrucker als auch Laserdrucker inzwischen sehr viel billiger produziert werden können als noch vor 5 Jahren denkbar.
Der Tintenstrahldrucker kann als Verwandter des Nadeldruckers gesehen werden. Der Unterschied liegt in der Tatsache, dass der Tintenstrahldrucker auf

elektrostatische Weise arbeitet. Ein winziger Tintentropfen wird unter hohem Druck durch kleine Düsen auf das Papier gespritzt und auf dem Weg zum Papier durch ein Hochspannungsfeld abgelenkt. Auch hier werden die Buchstaben aus einzelnen Punkten zusammengesetzt. Tintenstrahldrucker arbeiten leise und schnell. Durchschläge können wie beim Nadeldrucker nicht erstellt werden.
Auch Laserdrucker arbeiten berührungslos. Laserdrucker sind im Prinzip umkonstruierte Photokopierer. Sie bieten das beste Schriftbild und eignen sich auch für Graphiken. Sie können problemlos eine Auflösung bis 600 Punkte pro Zoll (Dots per inch - dpi) erreichen - d.h. fast Druckqualität. Da sie seitenorientiert arbeiten, verfügen sie in der Regel über einen (für Drucker) hohen Arbeitsspeicher. Tintenstrahl- als auch Laserdrucker können auch in Farbe ausdrucken - Farblaserdrucker sind sehr kostenintensiv.
Weitere, nicht so verbreitete Druckertypen sind LED-Drucker (Arbeitsweise ähnelt dem Laserdrucker) und der Thermodrucker (arbeitet mit speziellen Thermofarbbändern, die eine sehr gute Qualität liefern, aber hohe Kosten verursachen).

Plotter /vgl. Dic, S.81 ff./

Nadel-, Tintenstrahl-, Laserdrucker usw. können auch Zeichnungen ausdrucken. Wenn das Zeichnungsformat DIN A3 überschreitet, muss jedoch ein anderes Ausgabegerät verwendet werden. Wenn die Zeichnungen im wesentlichen aus Linien bestehen, also wenig Flächen beinhalten, dann sollten Plotter verwendet werden. Diese Geräte können sehr genau und farbig arbeiten. Sie sollen Zeichenstift(e) und Brett (bei Architekten und Ingenieuren) ersetzen. Es wird hier direkt mit einem Stift auf Papier, Karton oder Folie gezeichnet. Der Stift wird von Punkt A nach B geführt, d.h. vorher bestimmte Punkte werden mit einer Linie verbunden (vgl. Vektorverfahren). Der Antriebsmotor und die Zeitdauer des Stiftwechsels bestimmen die Zeichengeschwindigkeit des Plotters. Für Farbzeichnungen muss der Plotter eine programmgesteuerte Wechselvorrichtung für die Stifte haben. Es werden auch Plotter angeboten, die nach dem Prinzip des Tintenstrahldruckers arbeiten.

2.3 'eigentlicher' Rechner

Der eigentliche Rechner beinhaltet die Systemplatine und den Massenspeicher (eine oder mehrere Festplatten und/oder Diskettenlaufwerk(e)). Die schematische Darstellung der Systemplatine in Bild 2-4 zeigt ihren üblichen Aufbau mit Rechenwerk (Prozessor und Co-Prozessor), Arbeitsspeicher (RAM), Festspeicher (ROM)und Verbindungen zur Datenein- und -ausgabe.

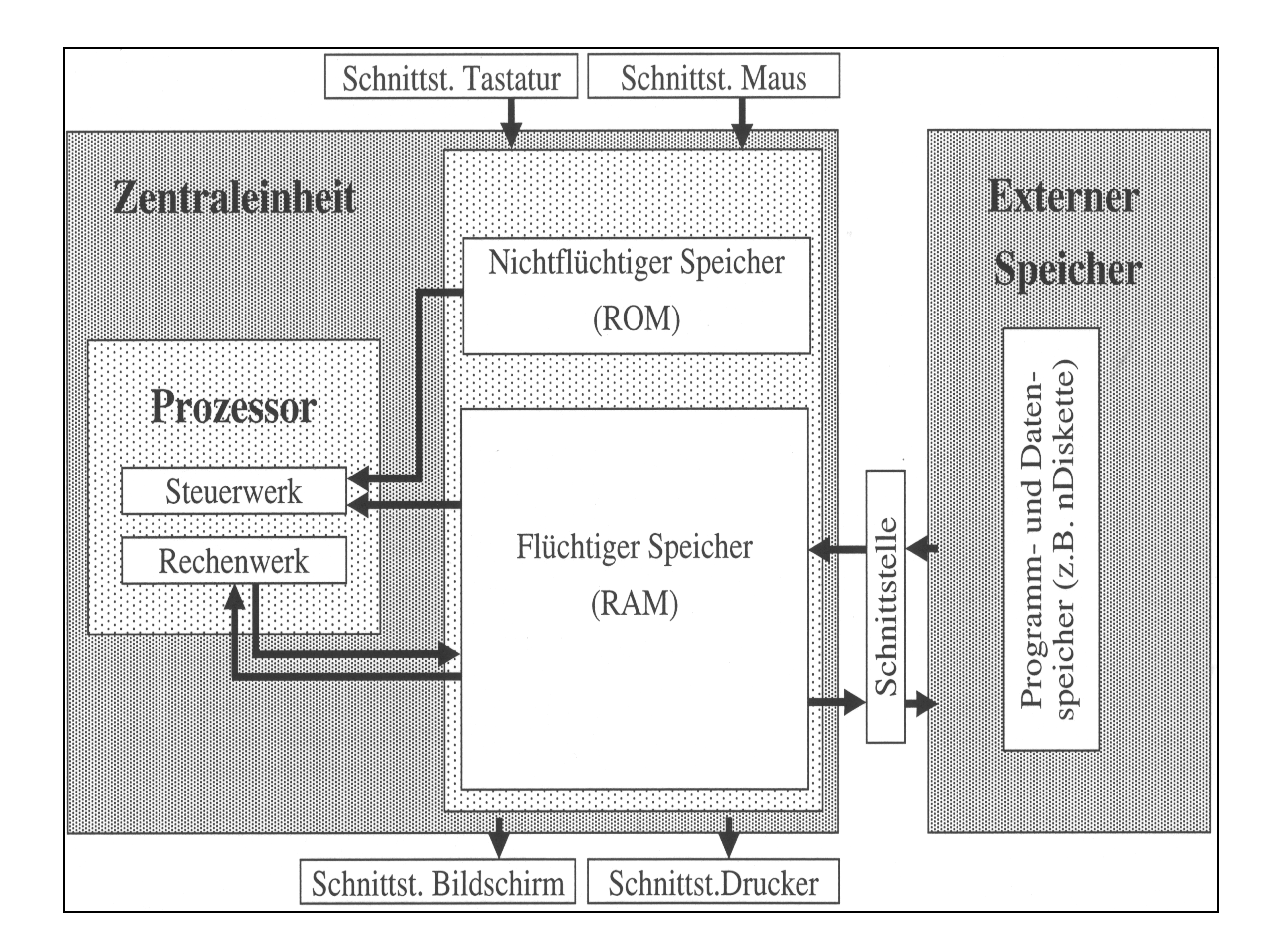


Bild 2-4 Zentraleinheit mit externen Speicher /Dic/

2.3.1 Massenspeicher /vgl. Imp, S. 190/

Massenspeicher lassen sich in Primär-, Sekundär- und Backup-Datenspeicher einteilen. Unter Primär-Datenspeicher werden Speicher verstanden, die Daten im Random Access, d.h. im direkten Zugriff auf Informationsblöcke, verfügbar halten. Zu dieser Gruppe gehören magnetische Festplattenlaufwerke. Man spricht auch von Winchesterplatten. Diese werden in unterschiedlichen Größen (von 2,5 bis 5,25 Zoll) mit entsprechend unterschiedlicher Kapazität angeboten. Ihre Speicherkapazität hat auch für PC-Anwendungen den Gigabyte-Bereich erreicht. Derzeit (Sommer 1999) werden entsprechend die PCs in der Regel mit Speicherkapazität im Gigabytebereich angeboten. Man kann davon ausgehen, dass die Festplatte den standardmäßigen Massenspeicher darstellt. Ihr großer Vorteil ist, dass sie den direkten Zugriff auf Daten aller Art ermöglicht.
Ähnlich wie Festplatten speichern die als Sekundär-Datenspeicher klassifizierten Massenspeicher die Daten. Ein direkter Zugriff auf die Daten ist erst dann gegeben, wenn das Speichermedium im Datenleser eingelegt ist. Zu dieser Klasse gehören magnetische und optische Wechselplattenlaufwerke, Diskettenlaufwerke

und Memory-Card-Drives. Wechselplattenlaufwerke werden gerne verwendet, wenn große Datenmengen von einem Rechner zum anderen transportiert werden sollen, ohne ein langwieriges Backup (Sicherungskopie einer größeren Datenmenge) zu ziehen. Auf dem Markt werden zwei Systeme angeboten:

- eine handelsübliche Festplatte wird in eine Wechselkassette eingebaut. Die kann dann komplett ausgetauscht werden.
- bei der klassischen Wechselplatte wird der Datenträger wie eine Diskette in das Laufwerk geschoben und dann genutzt.

Bekannter sind Disketten. Diese wurden im 5,25 Zoll und 3,5 Zoll Format vertrieben. Man kann sagen, dass das 3,5 Zoll Format die 5,25 Zoll Disketten verdrängt hat; sie sind kleiner, dadurch handlicher und auch stabiler und können mehr Daten speichern. Angeboten werden noch magneto-optische Platten (MO-Platten), WORM (Write once read multiple) -Platten und CD-ROMs (read only memory).

Bei MO-Platten handelt es sich um löschbare optische Platten. Hier ist kombiniert die Unempfindlichkeit optischer Platten, die Wiederbeschreibbarkeit von Magnetplatten und die Transportierbarkeit von Disketten.

WORM-Platten und CD-ROMs werden nur einmal beschrieben, können dann nur noch gelesen werden. Es handelt sich hierbei um Anwendungen der Lasertechnik.

Das typische Backupmedium ist der Streamer. Hierbei handelt es sich um ein Magnetbandlaufwerk mit hoher Speicherkapazität. Die Kosten sind recht gering, Speicherung und Zugriff auf die Daten ist jedoch zeitaufwendig. Seit einiger Zeit kann man auch als Endverbraucher CDs ‘brennen’. Die dafür notwendigen Geräte sind nicht (mehr) teuer. Daher wird die CD den Streamer als typisches Back-up Medium verdrängen.

2.3.2 'Interne' Speicher

Der interne Speicher wird auch als Hauptspeicher bezeichnet. Er beinhaltet einen fest programmierten Teil (Read Only Memory - ROM) und einen frei programmierbaren Teil (Random Access Memory - RAM). Bei DOS-Rechnern ist der ROM klein gehalten (ca. 16 Kbyte), bei Apple- Rechnern oder Atari-Rechnern liegt er bei ca. 200 Kbyte. Im ROM sind die Teile programmiert, die für die Inbetriebnahme des Rechners notwendig sind. Der frei programmierbare Speicher (RAM) ist bei DOS-Rechnern in mehrere Bereiche aufgeteilt. Es wird unterschieden in Hauptspeicher, Expanded Memory und Extended-Memory (vgl. Bild 2-5). DOS-Rechner können vom Betriebssystem aus gesehen nur 640 Kbyte verwalten.

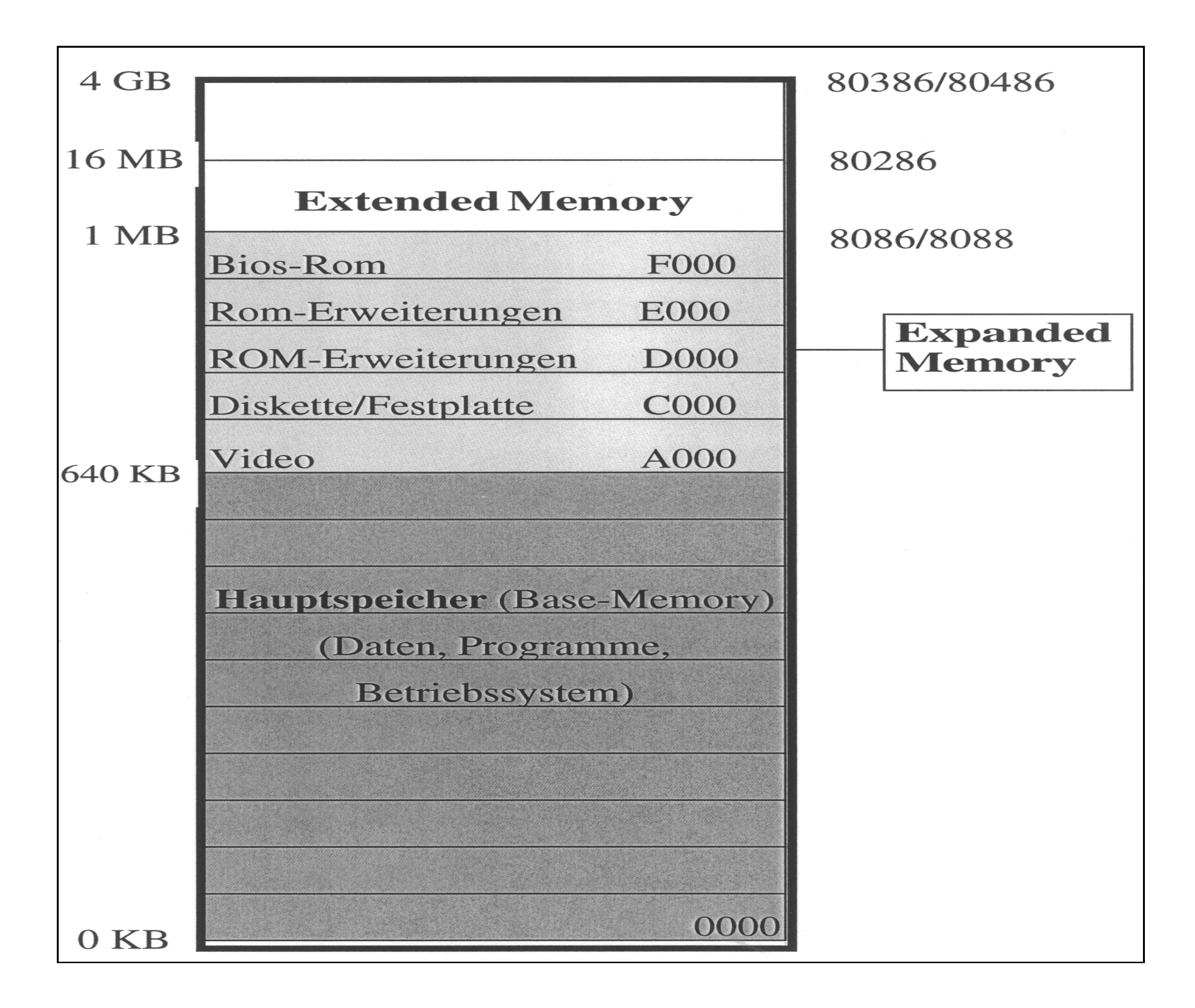


Bild 2-5 Aufteilung des Arbeitspeichers /Dic/

Neuere Software, insbesondere kombinierte Programme benötigen deutlich mehr Arbeitsspeicher. Dazu werden dann entweder der Expanded Memory oder der Extended Memory verwendet, je nachdem für welchen Speicher das Programm ausgelegt ist. Diese Dreiteilung des RAM ist bei Betriebssystemen wie OS/2, UNIX nicht notwendig. Auch Apple-Rechner kennen diese Dreiteilung nicht. Diese Betriebssysteme - auch WINDOWS - benötigen aber mehr als 1 Mbyte Arbeitsspeicher im Gegensatz zu einem DOS-Rechner, der damit auskommt. Standard sind im Sommer 1999 je nach Preisklasse zwischen 8 und 64 Mbyte Arbeitsspeicher, die Tendenz ist weiterhin steigend, da die Anwendungsprogramme immer umfangreicher und komplexer werden.

2.3.3 Prozessoren und Coprozessoren /vgl. Imp, S. 189 f., Dic, S. 31 ff./

Prozessoren werden als 'Hirn' oder als 'Herz' des Rechners bezeichnet. Der Mikroprozessor ist der Teil des Rechners, der die durchzuführenden Operationen rechnet und steuert. Er überprüft und bearbeitet jede Anweisung, die durchge-

führt werden soll. Die gebräuchlichsten Typen (für PCs) werden von Intel hergestellt. Ein moderner Prozessor verfügt über Steuerwerk, Rechenwerk und einen internen Speicher (Cache). Der Cache ermöglicht ein schnelleres Arbeiten als der externe Arbeitsspeicher an sich erlaubt. Dies ist bedingt durch die möglichen Taktfrequenzen, die innerhalb des Prozessors die 500 MHz - Grenze überschritten haben; bei der Peripherie liegt die Taktgrenze viel niedriger (um die 30 MHz)
Die Leistungsfähigkeit eines Prozessors wird durch die Adress- und Datenleitungen und durch den Systemtakt bestimmt. Mehrere parallele (Adress-, Steuer- oder Daten-) Leitungen bilden einen sogenannten Bus (vgl. Bild 2-6). Der Datenbus transportiert die Datenmengen; der Datenbus bestimmt also die Leistungsfähigkeit des Rechners.

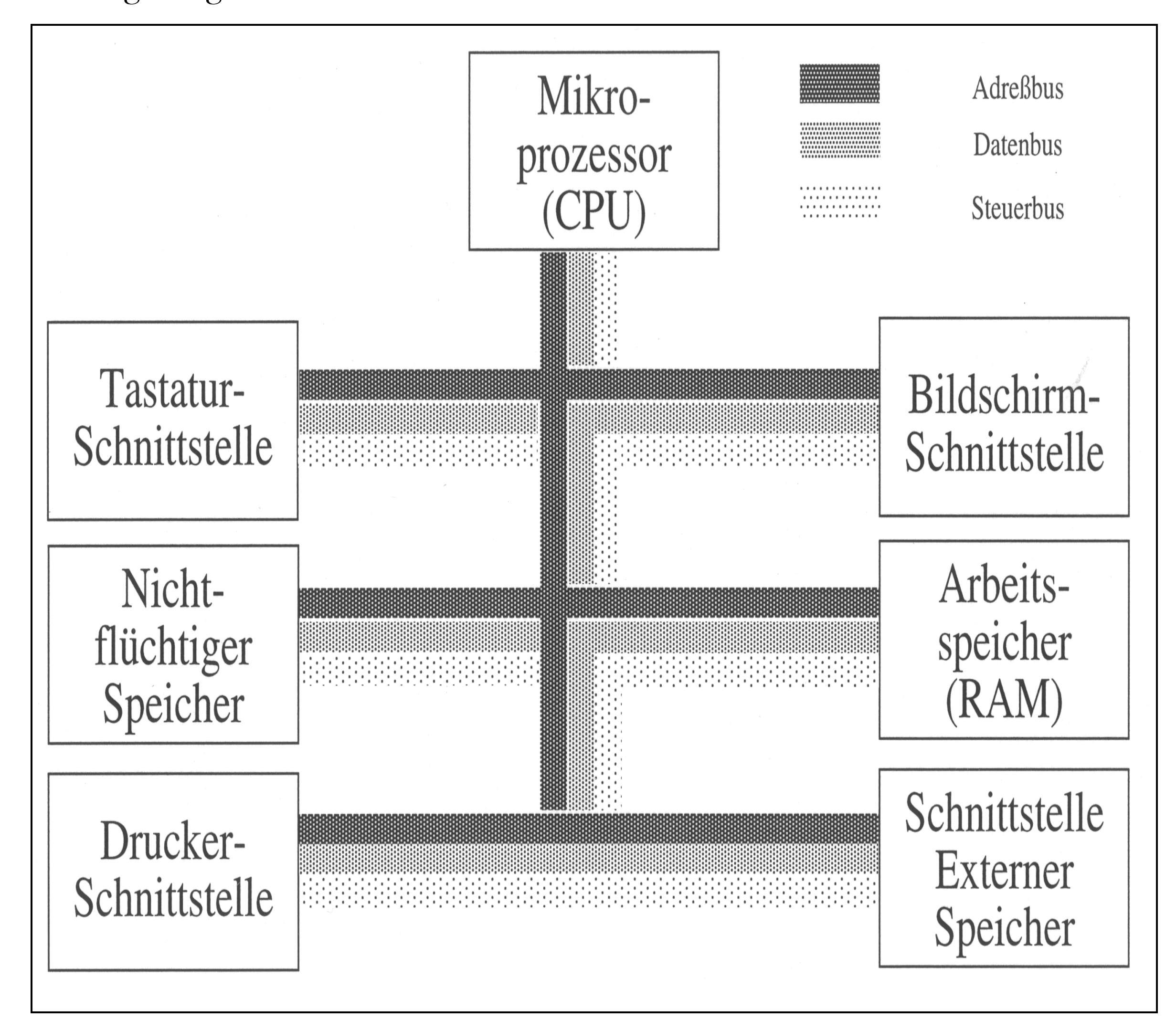


Bild 2-6 Der Systembus /Dic/

Die Zuordnung der Daten an den gewünschten Ort geschieht über den Adressbus, der Steuerbus regelt die Aktivitäten der Peripherie. Die Busbreite wird in Bit angegeben. Eine Leitung entspricht einem Bit. Je mehr parallele Leitungen (man spricht auch von der Breite) solch ein Bus hat, desto leistungsfähiger ist der Prozessor. Hierbei muss dann unterschieden werden zwischen internem Bus und externen Bus, die nicht immer gleich ausgelegt werden. Die interne Busbreite prägt auch die verarbeitbare Wortlänge. Da zur Darstellung eines Zeichens 8 Bit benötigt werden, kann die interne Busbreite nur acht Bit oder ein vielfaches von 8 Bit = 1 Byte sein. Das Spektrum der Prozessoren, die in PCs verwendet werden, reicht von einem Byte (8 Bit) bis acht Byte (64 Bit). Der Systemtakt der Prozessoren wird bereits bei der Fertigung auf eine bestimmte Frequenz beschränkt. Je höher der Systemtakt ist, desto schneller können Prozessorbefehle abgearbeitet werden. In Bild 2-7 sind verschiedene Prozessortypen mit ihrer Leistungsbeschreibung nebeneinandergestellt.

CPU-Typ	Transistoren in Millionen	Adressbus (bit)	Datenbus (bit)	Cache serienmäßig	Coprozessor	Bustakt (MHz)
8088		8	8		ext	4,77
80186		16	16		ext	10
80286	0,13	16	16		ext	bis 16
80386	0,28	32	32		ext	bis 33
80486	1,2	32	32	ja	int	bis 50
Pentium	3,1	32	64	ja	int	bis 250
Pentium II	7,5		64	ja	int	bis 450
Pentium III	9,5		64	ja	int	bis 600

Bild 2-7 Vergleich der verschieden Prozessoren (-entwicklungsstufen)

Eine weitere Möglichkeit, die Systemleistung von PCs zu steigern, ist der Einsatz von Coprozessoren. In der Regel werden mathematische Coprozessoren eingebaut. Diese führen Operationen mit Gleitkommazahlen ungefähr zehn bis hundertmal schneller aus als der dazugehörende Stammprozessor. Die Coprozessoren werden wie die Stammprozessoren bezeichnet, die letzte Ziffer ist jedoch eine Sieben. Auch die Taktfrequenz ist gleich.

2.3.4 Schnittstellen /vgl. Imp, S. 200 f./

Schnittstellen sind ein notwendiges Ausstattungsmerkmal der Rechner, da sie die Voraussetzung sind, dass externe Geräte an den Rechner angeschlossen werden können. Sie haben die Aufgabe acht Bit breite Datenblöcke vom Sender zum Empfänger zu übertragen. Dies kann parallel (d.h. acht Bit gleichzeitig) oder seriell (jeweils ein Bit nacheinander) erfolgen. Je nach Anwendungszweck haben sich verschiedene Schnittstellen als Standard etabliert; z.B. die Centronics-Schnittstelle als Druckeranschluss, die RS232 als Mausanschluss, wenn kein eigener Anschluss für die Maus vorgesehen ist. In Bild 2-8 werden die bekanntesten Schnittstellen zusammengefasst.

Schnittstellen

RS232

Sie wird in der Regel als bidirektionale Schnittstelle verwendet. Es ist eine serielle Schnittstelle. Es werden 9-polige oder 25-polige Verbindungen eingesetzt.

Centronics

Gilt als die am meisten verbreitete Schnittstelle. Ist eine // - Schnittstelle; d.h. alle 8 Datenbits werden gleichzeitig übertragen. In der Regel wird sie als Druckeranschluss benutzt. Ursprünglich unidirektional ausgelegt, wird sie immer häufiger bidirektional ausgelegt.

20-mA

Die 20-mA-Stromschleife wird auch als TTY (von Teletype = ASCII-Fernschreiber) bezeichnet. Logisch entspricht das Übertragungsformat der RS232. Zusätzlich wird ein 20-mA-Strom im Takt der Datenbits ein-ausgeschaltet.

RS422, RS423

Diese Schnittstellen sind für Datenübertragung auf größeren Entfernungen ausgelegt. Logisch entsprechen sie der RS232. Sie verwenden auch gleiche Kabel.

RS485

wie RS 422; hier können jedoch über nur zwei Leitungen mehrere Sender/Empfänger gekoppelt werden.

IEEE488

Hier können bis zu 15 Geräte mit einem Kabel miteinander verbunden werden. Ein einziges Gerät überwacht den Sendeverkehr. Wird häufig in der Messtechnik eingesetzt.

Bild 2-8 Schnittstellen; deren Besonderheiten

2.3.5 **Graphikkarten** /vgl. Imp, S. 199/

Um vom Rechner aus den Bildschirm steuern zu können sind Graphikkarten notwendig. Alte Rechner werden noch mit Monochrom Karten (z.B. Hercules Graphic Card - HGC) ausgestattet sein. Derzeit (1999) ist eine VGA- (Video Graphics Array) oder eine Super VGA- oder eine EGA- (Enhanced Graphics Adapter) Karte Standard. Hierbei handelt es sich um Karten zum Betrieb von Farbmonitoren.

2.4 Betriebssysteme /vgl. Dic, S.83 f./

Das Betriebssystem ist die notwendige Voraussetzung zum Betrieb eines Rechners. Ohne Betriebssystem kann der Rechner keine Befehle ausführen. Es ist abhängig von der CPU und teilweise im ROM-Speicher fest eingebrannt. Zumindest die Anweisungen zum 'Hochfahren des Rechners' und zum Einlesen des restlichen Betriebssystems von einem Massenspeicher aus müssen fest gespeichert sein. Daher wird das Betriebssystem von manchen zur Hardware gerechnet. Im allgemeinen wird es jedoch zur Software gezählt. Im Bild 2-9 ist dargestellt, wie die Betriebssysteme innerhalb der Software eingeordnet werden können.

Die Leistungsfähigkeit eines Rechners ist außer von der Hardware auch vom Betriebssystem geprägt. Der Datendurchsatz, die Datensicherheit und die Benutzerführung werden in hohem Maße durch das Betriebssystem festgelegt. Seine Aufgabe ist die Organisation der Vorgänge im Inneren des Rechners. Dies sind im einzelnen:

Definieren der Voreinstellung der Hardware nach dem Einschalten.

- Steuerung und Überprüfung der Eingabe über Tastatur, Maus, von externen - Speichern etc.
- Ebenso Steuerung und Überprüfung der Ausgabe zum Bildschirm, zu externen Speichern, zum Drucker usw.
- Suchen, Senden und Holen von Daten vom externen Speicher.
- Überprüfen freier Speicherplätze im internen und externen Speicher.
- Organisieren der Speicherung der Daten auf dem Datenträger.
- Steuerung des Programmablaufs.
- Überwachung und Steuerung der Zusammenarbeit der einzelnen Systemkomponenten.
- Das Betriebssystem versetzt den PC überhaupt erst in die Lage, Anwendungsprogramme abzurufen und mit ihnen zu arbeiten.

Rechnerprogramme (Software)

Betriebssystemsoftware Anwendungssoftware

Kommando-orientierte Betriebssysteme	***Grafikorientierte Betriebssysteme***	Standard-software - problem-orientiert	Branchen-software - branchen-orientiert	Individual-software

Persönliche Anwendung	Kommerzielle Anwendung	Baugewerbe	Nach den Angaben und Anforderungen des Auftraggebers erstellte Einzel-Programme
Textverarbeitung	Finanzbuchhaltung	Ärzte	
Projekt-Management	Budgetrechnung	Reisebüros	
Datenbank	Fakturierung	Versicherungen	
Desktop Publishing etc.	Lohn- und Gehaltsabrechnung etc.	Verlage Kfz-Handel usw.	

Bild 2-9 Klassifizierung der Software /nach Dic/

Betriebssysteme können klassifiziert werden nach der Zahl der Anwender, die das Betriebssystem bzw. den Rechner nutzen und nach der Anzahl der ablauffähigen Anwenderprogramme. Die Klassifizierung ist in Bild 2-10 dargestellt. Eine weitere Unterscheidungsmöglichkeit bietet die prinzipielle Arbeitsweise der verschiedenen Betriebssysteme. Man unterscheidet kommando- bzw. code-orientierte Betriebssysteme von grafisch orientierten Betriebssystemen . Gemeinsam ist beiden Systemarten, dass eine Dateistruktur mit Haupt- und Unterverzeichnissen aufgebaut werden muss. Typisches Beispiel für ein kommando-orientiertes System ist MS-DOS bis ausschließlich Version 4.01. Ab dieser Version wird auch eine Menüführung angeboten. Ein anderes Beispiel ist UNIX. Aber auch hierfür wird mittlerweile eine graphische Benutzeroberfläche angeboten. Das typische Beispiel für eine graphische Oberfläche ist das Betriebssystem der Apple Macintosh Rechner.

Folgende Betriebssysteme wurden/werden für Rechner der PC-Klasse angeboten:

- MS-DOS (Microsoft-Disc-Operating-System),
- PC-DOS (Personalcomputer-Disc-Operating-System)
- DR-DOS (Digital Research-Disc-Operating-System)
- OS/2 (Operating-System)
- GEM (Graphics Enviroment Manager) und WINDOWS (benötigen beide DOS)
- Unix (Linux)
- Herstellerabhängige Systeme wie von Apple Macintosh, Commodore und Atari

Betriebssysteme			
Einplatzsystem (Single-User)		Mehrplatzsystem (Multi-User)	
Einaufgaben-system (Single-Tasking)	Mehraufgaben-system (Multi-Tasking)	Einaufgaben-system (Single-Tasking)	Mehraufgaben-system (Multi-Tasking)

Bild 2-10 Klassifizierung der Betriebssysteme /Dic/

2.5 Netzwerke /vgl. Dic und Tro/

Als Fachkraft für Arbeitssicherheit wird man in manchen Fällen für seine Arbeit Daten benötigen, von denen bekannt ist, dass sie auf einem anderem Rechner abgespeichert sind. Es kann vorkommen, dass diese Daten nicht auf Papier benötigt werden, sondern als Datei, um im Rechner weiterverarbeitet zu werden. Bei solchen Gegebenheiten ist es vorteilhafter, nicht einen 'Stand Alone PC' anzuwenden, sondern einen Anschluss an andere Rechner zu haben; oder wenigstens die Möglichkeit dazu, solch einen Anschluss herzustellen. Werden mehrere Rechner zusammengeschlossen, spricht man von Netzwerken. Mit Netzwerken können verschiedene Ziele verfolgt werden:

- Zugriff auf im zugreifenden Rechner nicht gespeicherte Daten, da
- -- die Daten zentral gespeichert sind,
- -- die Daten auf mehrere Rechner verteilt sind oder
- -- die Daten im Rechner einer anderen Abteilung sind.

- Zugriff auf im zugreifenden Rechner nicht vorhandene Programme, da
- -- die Programme zentral gelagert sind,
- -- die Programme mehr Arbeitsspeicher benötigen, als der Rechner hat. D.h.
- -- es wird auf die Verarbeitungskapazität anderer Rechner zugegriffen.
- Zugriff auf Peripherie-Geräte wie
- -- zentraler Drucker,
- -- zentraler Plotter,
- -- zentraler Backup-Speicher da dadurch
- -- teuere Endgeräte (z.B. Farblaserdrucker) mehrfach genutzt werden können.
- Nachrichten können ausgetauscht werden, entweder
- -- direkt oder
- -- über Mailbox.
- Bei Verwendung von PCs können einfacher ausgestattete PCs ihre Anwendungsmöglichkeiten steigern.

Anm.: Bei der Verwendung von PCs als Teilnehmer behalten diese ihre Rechenkapazität und können diese für individuelle Anwendungen weiterverwenden.

Als FaSi kann man davon ausgehen, dass man für ein Rechnernetz selbst nicht verantwortlich ist, jedoch in der Lage sein sollte, dieses anzuwenden und die vorhandenen Möglichkeiten kennen sollte. Man führt in der Regel als FaSi Netze nicht selbst ein, sondern bekommt dergleichen am Arbeitsplatz vorgegeben, bzw. bekommt einen Anschluss an diese - wenn sie vorhanden sind.
Gesetzt den Fall, ein Netz (es wird auch von Rechnerverbund gesprochen) ist nicht vorhanden und soll eingeführt werden. Dies ist dann eine Aufgabe, bei der sich die FaSi mit einschalten sollte - auch im Eigeninteresse, um möglichst viele Vorteile aus einem Netzbetrieb zu haben. Daneben sollte die FaSi etwas auf die anfallenden Probleme der Datensicherheit und des Datenschutzes achten (an sich Aufgabe des Datenschutzbeauftragten).
Daher sollte die FaSi neben den schon erwähnten Zielen eines Rechnernetzes auch etwas über die Rechnernetze selbst wissen.
Vier verschiedene Netzwerkklassen können unterschieden werden:

Gliederungsgrundlage ist die natürliche Ausdehnung der Netze:

GAN = Global Area Network

Dieses Netz arbeitet weltumspannend und verbindet die Rechner auf verschiedenen Kontinenten miteinander. Üblicherweise verwendet dieses Netz

einen Satelliten zum Datentransport. GAN-Netze können sowohl öffentliche Netze als auch firmeneigene Netzwerke sein, zum Beispiel VNET von IBM.

WAN = Wide Area Network

Mit diesem Netz sind die Rechner in einzelnen Ländern innerhalb eines Kontinents oder innerhalb der Landesgrenzen miteinander verbunden. Das Transportieren der Daten übernimmt hier ein Metall- oder Glasfaserkabel. Mit einem Zwischennetzkoppler können WAN-Netze zu GAN-Netzen gekoppelt oder selbst GAN-Netze werden. Beispiel für WAN -Netze sind : Die verschiedenen öffentlichen Dienstnetze der Telekom (Datex-, Telefon- und Direktrufnetz bzw. das neue ISDN-Netz, EURONET usw.)

MAN = Metropolitan Area Network

Sie sollen zukünftig innerhalb eines Stadtgebietes (Ballungsraumes) den Netzwerkbedarf abdecken. Man verspricht sich davon eine höhere Übertragungsgeschwindigkeit als bei den WAN-Netzen. Diese Netzart wird vor allem in den USA eingesetzt (zum Beispiel im Ballungsraum Los Angeles) und ist für Deutschland weniger interessant.

LAN = Local Area Network

Diese Netze sind nur lokal innerhalb einer Grundstückgrenze oder eines Firmengeländes erlaubt und zählen nicht mehr zu den öffentlichen Netzen, daher unterliegen sie auch nicht mehr deren Vorschriften. Zum Datentransport verwendet man überwiegend ein Koaxial- oder Glasfaserkabel. LAN-Netze können direkt oder über WAN oder MAN miteinander verbunden werden. Beispiele hierfür sind IBM-Token-Ring, Ethernet usw.

Auf die Technik der ersten drei Netzwerkklassen wird nicht eingegangen, da dies für eine FaSi unrelevant ist. Es wird in Kapitel 2.6 das Internett vorgestellt und kurz auf die Datennetze und Dienste der Telekom eingegangen, da diese im allgemeinen Gebrauch sind - trotzdem nicht immer bekannt sind. Sie sind in Bild 2-11 zusammengestellt. Erwähnenswert ist, dass die Telekom von der Bundespost ein analoges Netz und in weiten Bereichen ein zweites, digitales Netz übernommen hat. Das analoge Netz dient i.d.R. zum Telefonieren und als Telefaxleitung. Das digitale Netz wird verwendet für Internet, Telex, Telefax und Datex. Die Übertragungsleistung beim analogen Netz liegt zwischen 200 - 4800 Bit/s, beim digitalen Netz liegt sie bei 50 - 48000 Bit/s. Das analoge Netz gilt als störanfällig und ist gut abhörbar. Das digitale Netz ist deutlich weniger störanfällig und die Datensicherheit ist besser gewährleistet - d.h. es ist nicht so gut abhörbar. Es ist schneller, gilt als qualitativ besser und soll billiger sein.

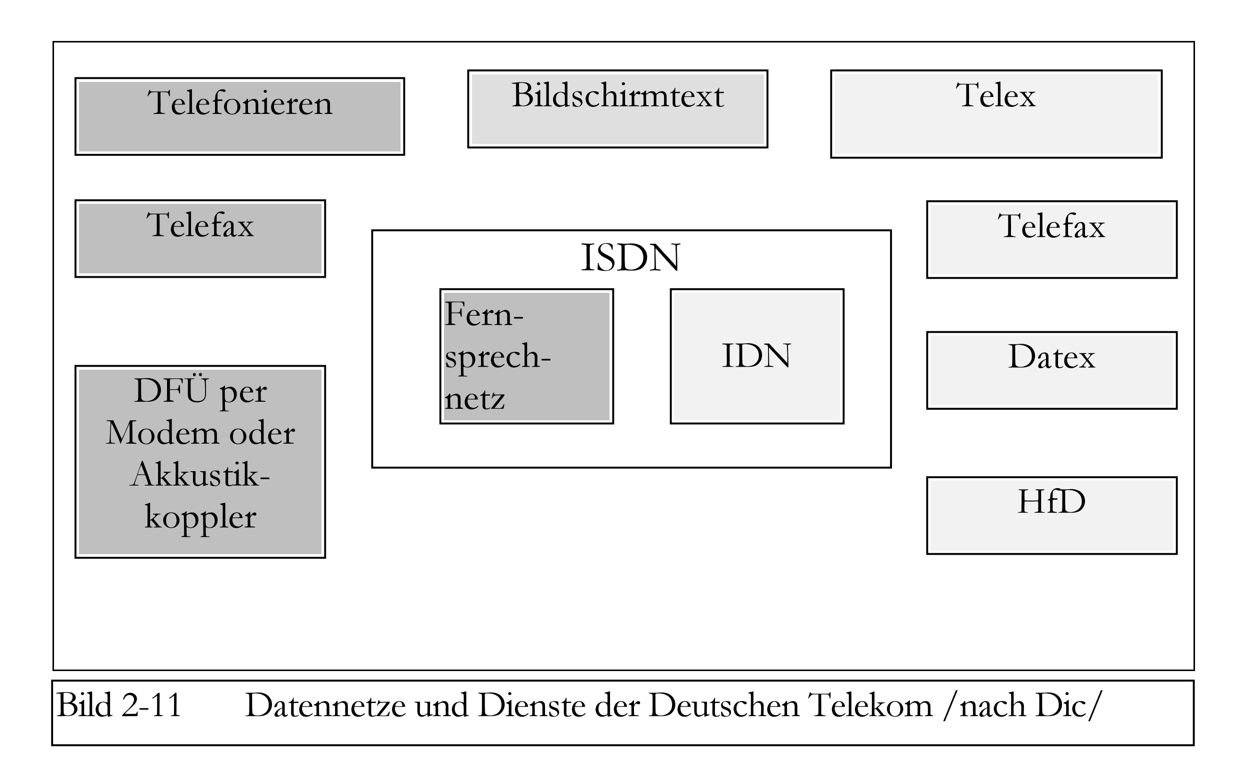


Bild 2-11 Datennetze und Dienste der Deutschen Telekom /nach Dic/

2.5.1 Kennzeichen lokaler Netzwerke (LAN)

Ausführlich soll auf LANs eingegangen werden. Insbesondere Konzerne, Verwaltungen, Forschungseinrichtungen und Bibliotheken verfügen in der Regel über hausinterne Rechnernetze. Es kann davon ausgegangen werden, dass auch eine FaSi immer häufiger LANs anwenden wird.

Mit Hilfe der Definitionen, die zum einen Gihr (1986 auf dem Telematica-Kongress) und zum anderen die ISO geben, kann man die Eigenschaften der LANs beschreiben:

Definition der International Standard Organisation:

"Ein lokales Netzwerk dient der bitseriellen Informationsübertragung zwischen miteinander verbundenen unabhängigen Geräten. Es befindet sich vollständig im rechtlichen Entscheidungsbereich des Benutzers und ist auf sein Gelände beschränkt."

Definition nach Gihr, 1986 auf dem Telematica-Kongreß:

"Unter lokalen Netzwerken (Local Area Network, LAN) werden spezielle Kommunikationsnetze verstanden, welche durch eine eng begrenzte räumliche Ausdehnung von nur wenigen Kilometern, ein gemeinsames breitbandiges Übertragungsnetz sowie eine dezentrale Steuerung gekennzeichnet sind. LANs eignen sich besonders gut zur Vernetzung von Rechnern, Arbeitsplatzsystemen (Workstations), [...] u.a.m., zwischen denen kurzzeitig große Datenmengen ausgetauscht werden müssen."

Unter Verwendung der Stichworte Ausdehnung, Topologie, Übertragungsmedium, Steuerung, Datenformate und beteiligte Stationstypen wird eine Beschreibung von lokalen Netzwerken nach Troitsch /Tro/ gegeben.

1. ***Ausdehnung***

   LANs dienen in der Regel der Verbindung von Rechnersystemen in einem Gebiet, das (in Deutschland besonders wichtig) nicht der Posthoheit unterliegt. Daher ergibt sich eine Beschränkung auf Gebäude oder Grundstücke - also auf Entfernungen von typisch kleiner fünf Kilometer.

   Größere Ausdehnungen lassen sich bei Bedarf durch Kopplung zweier Netzwerkteile über eine festgeschaltete Verbindung erzielen, wobei gelegentlich auch Postleitungen mit im Spiel sind.

2. ***Topologie***

   Die Netztopologie, die Art und Weise der Verbindung der einzelnen Netzteilnehmer also, beschränkt sich bei lokalen Netzen im wesentlichen auf die drei Grundformen Ring, Bus und Stern.

3. ***Übertragungsmedium***

   Im Gegensatz zu Fernnetzen (Wide Area Networks, WAN), die oft immer noch auf Fernmeldewege mit in der Regel maximal 64 kBit/s als Übertragungsrate angewiesen sind, wird in LANs immer ein Übertragungsmedium mit hoher Übertragungsrate (typisch zwischen 1 und 10 MBit/s) verwendet.

   Die konkrete Ausführung des Übertragungsmediums sowie die Übertragungstechnik (Basis- oder Breitband) ist von Netzwerk zu Netzwerk unterschiedlich. Die verschiedenen Übertragungsmedien sind:

- **Verdrillte Zweidrahtleitung**

♦ Zeichnet sich aus durch seine Preiswürdigkeit, es ist einfach zu verlegen, Abschlusswiderstände oder Abknickwinkel müssen nicht berücksichtigt werden. Bereits verlegte Telefonleitungen können verwendet werden.

♦ In der Regel geringe Übertragungsgeschwindigkeit (1MBit/s), empfindlich gegen Störfelder, nicht abhörsicher.

♦ Durch Abschirmung kann die Geschwindigkeit gesteigert werden, der Preisvorteil entfällt dann.

- **Koaxialkabel**

♦ Bietet hohe Übertragungsgeschwindigkeit, hohe Störsicherheit (i.allg. ausreichend für die Praxis).

♦ Deutlich teuerer als Zweidrahtleitung, erfordert sorgfältiges Verlegen. Knicke, Verdrehen, fehlende Abschlusswiderstände können sich störend auswirken.

- **Lichtwellenleiter**

♦ Gelten als vollständig störsicher, der Übertragungsgeschwindigkeit ist nach oben keine (praktisch ernst zu nehmende) Grenze gesetzt (einige hundert MBit/s). Unbemerktes Einkoppeln in dieses Medium kann ausgeschlossen werden.

♦ Sehr hoher Preis, daher beschränkt auf Spezialbereiche mit starken Störfeldern oder extremen Datensicherheitsanforderungen

Bei den **Übertragungsverfahren** kann unterschieden werden zwischen Basisband- und Breitbandverfahren. Beim Basisbandverfahren werden alle Daten direkt aufs Netz gegeben. Es können alle aufgezählten Kabelarten verwendet werden. Hingegen werden bei einem Breitbandverfahren die Daten auf einen Zwischenträger abgelegt, der eine erhöhte Übertragungsmöglichkeit bietet. Es können dann aber nur Koaxialkabel und Lichtwellenleiter verwendet werden.

4. Steuerung

Herkömmliche Kommunikationsnetze (Fernnetze) verfügen für die Kommunikation im Netz in aller Regel über sogenannte Knotenrechner. Hierbei handelt es sich quasi um Vermittlungsstellen, welche die Daten des Senders innerhalb des Netzes an den Empfänger weiterreichen und dabei eine optimale Wegauswahl durchführen. Der reibungslose Ablauf der Übertragung zwischen den Endstellen und den Knotenrechnern und auch zwischen den Knotenrechnern untereinander erfordert eine spezielle Steuerung, die zentral (durch einen eigenen Knotenrechner) oder dezentral (durch die Zusammenarbeit aller Knotenrechner) erfolgen kann.

Lokale Netze haben im Vergleich zu Fernnetzen eine recht einfache Topologie ohne solche Knotenrechner. Stattdessen sind alle beteiligten Stationen an ein und dasselbe Übertragungsmedium gekoppelt und "jeder kann mit jedem" Daten austauschen. Aus diesem Grund benötigen lokale Netze keine Flusssteuerung im eigentlichen Sinn. Die allerdings noch erforderlichen Kontrollen, *wer* das Übertragungsmedium *wann* benutzen darf, werden lokal unter der Steuerung eines entsprechenden Zugriffsverfahrens von den einzelnen Netzwerkstationen übernommen. Durch dieses Zugriffsverfahren wird festgelegt, wer

- Daten senden darf,
- wann diese Daten gesendet werden dürfen,
- wer diese Daten empfangen darf und
- wann die Daten empfangen werden (dürfen).

Die gebräuchlichsten Verfahren sind das 'Carrier Sense Multiple Access mit Collision Detection' (CSMA/CD-Verfahren) und das Token Passing (Token Ring).

5. ***Datenformate***

Die Übertragung der Nachrichten innerhalb des Netzes erfolgt in LANs (wie auch in Fernnetzen) praktisch ausschließlich in Blöcken oder "Paketen" (auch "Frames").

Den prinzipiellen Aufbau eines solchen Datenblockes zeigt Bild 2-12. Auf den ersten Blick einsichtig ist der Zweck derjenigen Komponenten, die Empfängeradresse, Daten und Prüfsumme enthalten. Die Absenderadresse wird für die Rückmeldung über den korrekten (oder auch fehlerhaften) Empfang der Daten benötigt, während die Folgenummer die richtige Montage einer für die Übertragung zerteilten Nachricht ermöglichen soll. Die Bedeutung der zusätzlichen Steuerinformationen ist vom jeweiligen Netz und seinen Eigenschaften abhängig.

Synch	Steuer-information	Absender Adresse	Empfänger Adresse	Folge-nummer	Nutzdaten	Prüf-summe

Bild 2-12 Aufbau eines Datenpaketes (schematisch)

6. ***Beteiligte Stationstypen***

Typischerweise sind in lokalen Netzen Rechnersysteme, Ein- und Ausgabegeräte, Speichermedien und oft noch spezielle Peripheriegeräte etwa für die Prozess-Steuerung zusammengeschlossen.

Fernnetze hingegen verbinden in aller Regel nur Rechner untereinander bzw. Rechner mit Terminals. Ein Zugriff über ein Fernnetz (mit einer Übertragungsrate von z. B. 1 kByte/sec) auf einen entfernt stehenden Plattenspeicher gäbe auch nicht viel Sinn, während im lokalen Netz durch die hohe Übertragungsrate ein gemeinsamer Zugriff auf einen zentralen Massenspeicher durchaus praktikabel ist.

Mit Hilfe dieser sechs Kriterien lassen sich lokale Netzwerke bereits recht gut charakterisieren und von anderen Netzen abgrenzen. Die Netzwerke, die als LAN ausgelegt sind, unterscheiden sich also im wesentlichen in den vier Grundkriterien

- **Topologie**
- **Übertragungsmedium**
- **Übertragungstechnik**
- **Flusssteuerung / Zugriffsverfahren**

Für die drei anderen Kriterien, die für Netzwerke allgemein interessant sein können, gilt:

- Die **Ausdehnung** ist (wenn überhaupt unterschiedlich) durch das Übertragungsmedium und das Übertragungsverfahren bestimmt (durch Probleme mit Leitungsdämpfung bzw. Laufzeiten).
- Die **beteiligten Stationstypen** werden durch die Anwendung des Netzes und durch die Auslegung des Netzwerkbetriebssystems festgelegt.
- **Datenformate** sind ein Problem der "untersten Ebene" des Netzwerksystems und sollen hier nicht in Betracht gezogen werden. Die Tatsache, dass die Daten grundsätzlich in Blöcke zerlegt werden, bevor sie übertragen werden können, reicht für das Verständnis völlig aus.

2.5.2 Aufgaben lokaler Netzwerke

Die Aufgaben der LANs werden in folgenden Stichworten beschrieben:

- **Nachrichtenaustausch**
  - ♦ Übermittlung einzeiliger Nachrichten
  - ♦ 'Electronic-Mail' - System
- **Zugriff auf zentrale Betriebsmittel**
  - ♦ Plattenspeicher
  - ♦ Drucker
  - ♦ Plotter
- **Zugriff auf die Verarbeitungskapazität anderer Rechner**
  - ♦ Abgabe von Aufträgen zur Stapelbearbeitung
  - ♦ Übergabe spezieller Rechenoperationen an einen Spezialprozessor
  - ♦ Zusammenfassen zweier Rechner zu einem Bildverarbeitungssystem
- **Zugriff auf zentrale Datenbestände**
  - ♦ Dies kann sich um einen Zugriff auf Datensätze handeln
  - ♦ I.d.R. wird gleichzeitig das dazu notwendige Programm mitbenutzt
  - ♦ Problem des sogenannten 'Record-Lockings'

Zum

Nachrichtenaustausch

ist anzumerken, dass hierunter einerseits eine einfache Übermittlung von einzeiligen Nachrichten an Benutzer, die gerade arbeiten, zu verstehen ist. Die abgesandte Nachricht erscheint am Bildschirm des Empfängers, wird aber in der Regel nirgendwo zwischengespeichert.

Auf der anderen Seite kann unter dem Begriff Nachrichtenaustausch auch ein komplettes "Electronic-Mail"-System verstanden werden. Hier können komplette Texte an andere Benutzer des Netzes versandt werden. Sie bleiben solange gespeichert (in einem elektronischen Briefkasten), bis der Empfänger sie liest und dann selbst anderweitig abspeichert, ausdruckt oder löscht. Ein solcher Austausch von Dateien ist nicht nur auf Briefe beschränkt; im Prinzip kann so jede beliebige Datei-Art von Benutzer zu Benutzer übertragen werden. Das Stichwort hierzu lautet File-Tranfer. Der

Zugriff auf zentrale Betriebsmittel

ist notwendig, weil die einzelnen Benutzerstationen in einem LAN in der Regel nicht über das volle Spektrum von Peripheriegeräten wie Magnetplatten, Bänder, Drucker, Plotter usw. verfügen.

Eine wichtige Aufgabe des LAN ist es daher, alle im Netz vorhandenen Peripheriegeräte allen Benutzern zugänglich zu machen. Dies gilt insbesondere für zentrale Plattenspeicher sowie für Spezial-Peripherie, die nicht problemlos an jede Station angeschlossen werden kann (und sei es auch nur aus Kostengründen). Diese Aufgabe des LAN wird häufig auch als "Resource-Sharing" bezeichnet, also als gemeinsamer Zugriff auf zentrale Betriebsmittel. Zum

Zugriff auf die Verarbeitungskapazität anderer Rechner

ist zu bemerken, dass LANs im Prinzip auch die Möglichkeit bieten, Verarbeitungsaufträge innerhalb des Netzes auf andere Rechner auszulagern (man spricht von einem Lastverbund). Dies kann im einfachsten Fall die Übergabe eines kompletten Auftrages an einen speziellen Rechner sein, der diesen per Stapelverarbeitung abarbeitet. Denkbar ist aber auch die Übergabe spezieller Rechenoperationen an einen Spezialprozessor, der in das Netz integriert ist. So lassen sich zum Beispiel zwei Rechner zur Darstellung bzw. Bearbeitung von Bild-Daten in einem Bildverarbeitungssystem durchaus in einem LAN zusammenfassen. Wichtig ist auch der

Zugriff auf zentrale Datenbestände

Diese Aufgabe ist die weittestgehende von allen: Hier soll nun nicht nur ein Gerät oder eine CPU innerhalb des Netzes von verschiedenen Stationen aus benutzt werden - stattdessen stellt ein zentrales System (ein Server) eine Datenbank und ein zugehöriges Verwaltungsprogramm zur Verfügung, das allen Benutzern des Netzwerkes einen Zugriff auf diese zentralen Daten ermöglicht, und zwar auf der Ebene des Datensatzes oder Datenfeldes.

Hauptproblem ist hier die Synchronisation von gemeinsamen Dateizugriffen, das sogenannte Record Locking. Wenn zwei Stationen gleichzeitig auf denselben Datensatz schreibend zugreifen wollen, so muss die Verwaltungssoftware in der Lage sein, diese Konkurrenz-Situation (z. B. durch eine Zugriffssperre für einen der beiden) zu behandeln.

2.6 Das Internet /nach Kir/

Das Internet ist ein weltumspannendes Computernetz mit vielen Millionen Teilnehmern. Ursprünglich war es ein Netzwerk des US-amerikanischen Verteidigungsministeriums (ARPAnet), welches dann auf die amerikanischen Universitäten ausgedehnt wurde (NSFnet). Nun sind nicht nur Bildungseinrichtungen, sondern auch unzählige kommerziell betriebene Server weltweit angeschlossen. Die für eine FaSi interessantesten Internet-Dienste sind:

- E-Mail (email, electronic mail, elektronische Post)
- World Wide Web (WWW)

„Das E-Mail ist der "fundamentale" Internet-Dienst. Sie dient zunächst dem direkten Informationsaustausch zwischen Internet-Teilnehmern und ist erheblich schneller als die "gelbe Post", jedoch nicht so direkt wie ein Telefongespräch, kann aber dafür quasi die Funktion eines Anrufbeantworters mit übernehmen.

Weiterhin kann E-Mail über Mailing-Listen auch dem Informationsaustausch zwischen größeren Personengruppen dienen, und schließlich kann sie auch als Ersatz für andere Internet-Dienste wie Dateiübertragung (FTP) oder "World Wide Web" herangezogen werden.“ /Kir/

Das World Wide Web (WWW) „ist ein weltweites, auf Hypertextdokumenten basierendes Informationssystem. Hypertextdokumente enthalten Verweise (Anm. des Autors: „Link“) auf weitere Dokumente, die man dann durch einen Mausklick oder einen Tastendruck bequem erreichen kann. Die Texte enthalten Formatierungsmerkmale und Schriftattribute und sind deshalb angenehm lesbar, ferner ist das System multimediafähig, das heißt, Graphiken, Bilder, Videos und Klänge können übermittelt werden. Es ist auch ohne weiteres möglich, WWW-Dokumente über ein nicht-graphikfähiges Textterminal zu lesen.“ /Kir/

Das Internet bietet einer FaSi eine enorme Menge von Informationen. Viele Computerprogramme, die als "Public Domain"-Programme kostenfrei angeboten werden, sind auch für eine FaSi nützlich, auch Shareware-Programme (Hier erwartet der Autor nach Ablauf einer Probezeit ein gewisses finanzielles Entgelt.) können von Interesse sein.

Die deutschen Hochschulen waren schon früh über die Rechenzentren über das Wissenschaftsnetz (WIN) mit dem Internet verbunden. Inzwischen sind auch oft die einzelnen Universitätsinstitute mit dem Internet direkt verbunden. Ebenso haben viele Betriebe, Institutionen und Behörden einen direkten Internet Anschluss. Als Privatmann kann man ebenfalls auf das Internet zugreifen. Man kann sich über ein Modem (In neueren Computern ist dies bereits eingebaut) und das Telefonnetz oder über ISDN (Integrated Services Digital Network, 64 KBit/s) unter Vermittlung eines Netzwerkanbieters in das Internet einwählen. Wenn man das Glück hat Hochschulangehöriger zu sein, kann man sich in der Regel an das Hochschulrechenzentrum wenden, anderenfalls muss man einen der zahlreichen kommerziellen Netzwerkanbieter konsultieren.

2.6.1 Details zu Electronic Mail (E-Mail, email)

„Elektronische Post, meist Electronic Mail oder E-Mail genannt, dient zum Verschicken von Briefen über Computernetze. Es handelt sich um den bekanntesten und am meisten genutzten Kommunikationsdienst auf Rechnersystemen, über den weltweit –zig Millionen Teilnehmer, insbesondere Universitätsangehörige, erreichbar sind. E-Mail bietet gegenüber der klassischen Kommunikation mit Hilfe der "gelben Post" einige Vorteile: sie ist sehr schnell, preiswert und einfach handhabbar.
E-Mail ist nicht auf das Internet beschränkt. Es gibt Schaltstellen (Gateways) zu anderen E-Mail-Netzen wie z.B. BITNET, EAN, CompuServe.
Zum Verschicken einer E-Mail ist die exakte Kenntnis der Zieladresse des Empfängers notwendig. Die Adresse muss in einer speziellen Form angegeben werden; ***weder Tippfehler noch Auslassungen werden verziehen, es erfolgt keine automatische Korrektur.***
Eine E-Mail-Adresse im Internet sieht beispielsweise wie folgt aus:

schulze@physik.uni-heidelberg.de

Mit dieser Adresse würde man den (hypothetischen!) Benutzer Schulze an einem Computer des Fachbereichs Physik der Universität Heidelberg in Deutschland erreichen. ...
Der Textkörper kann beliebigen ("ASCII"-) Text enthalten. Angemerkt sei, dass die Verwendung deutscher Umlaute Probleme bereiten kann, da es verschiedene Codierungen gibt, die beim Empfänger nicht unbedingt richtig ankommen bzw. umgesetzt werden.
Typische E-Mail-Benutzerprogramme haben etwa folgenden Leistungsumfang: Selektives Lesen eingegangener E-Mails, Archivieren, Export, Drucken, Beantworten (reply), Weiterschicken (forward) und Löschen; Schreiben eigener

E-Mails (compose), ggf. unter Verwendung vorgefertigter Texte und, wenn gewünscht, mit Kopie (Cc:) an weitere Adressaten."/KIR/
E-Mail-Benutzerprogramme werden für alle gängigen Computertypen angeboten. Für Intel-PCs war/ist beispielsweise `pmail = Pegasus Mail´ sowie `Netscape´ sehr verbreitet.

2.6.2 Details zum World Wide Web (WWW)

Will man das weltweite Hypertext-Informationssystems "World Wide Web" (WWW) benutzen ist neben einem Internetzugang auch ein Benutzerprogramm notwendig. Dies nennt man Browser. Von vielen bevorzugt wird der Browser Netscape. Für alle gängigen Computersysteme wie Unix-Workstations, Intel-PCs und Apple Macintosh gibt es WWW-Browser.
„Die Benutzung dieses Informationssystems ist prinzipiell kinderleicht. Um einem Verweis zu folgen, braucht man nur ein markiertes Wort oder Symbol einmal mit der Maus anzuklicken. Die Markierung wird z.B. durch blaue Farbgebung und Unterstreichung kenntlich gemacht. Die Sprünge sind im WWW zwar nur in einer Richtung möglich, die Browser gestatten aber auch den Rücksprung zum letzten Dokument oder eine Navigation innerhalb von "History" oder "Hotlist". Das WWW-System bietet volle Multimedia-Unterstützung wie Graphik, Bilder, Ton und Video." /Kir/
Das WWW hat sich zu einer Informationsquelle erster Güte entwickelt. Als FaSi findet man fast alles an Information, die bei der täglichen Arbeit als auch in besonderen Fällen benötigt wird. Insbesondere zu Gefahrstoffen, Abfallproblemen, Rechtsgrundlagen und Ergonomie bieten die Web-Seiten von öffentlichen Instanzen (Bundes- und Landesregierungen, BGen, Hochschulen) und von privaten Verbänden und Betrieben (VDSI, VDI, Gewerkschaften) eine Fülle von nützlichem, aktuellem und oft wichtigem Wissen. Im Anhang werden verschiedene Web-Seiten und ihre Themenbereiche aufgeführt. An sich würde es reichen, nur ein oder zwei Adressen anzugeben. Über Links (Verweise, Hyperlinks – den in der Regel blau oder Rot markierten Text einfach anklicken) findet man dann zu den verschiedenen Seiten, die für eine FaSi wichtig sein können. Leider ist jedoch oft nicht angegeben, was der Inhalt ist oder wo der Schwerpunkt dieser Seite liegt, ob die Seite einen „interaktiven Dialog" ermöglicht, also eine direkte Datenbankfunktion ermöglicht und ob die Informationen kostenpflichtig sind oder nicht.
„Ein gegenwärtig diskutiertes Thema ist das Gebiet des "Electronic Publishing". Das WWW-System eignet sich bestens dazu, wissenschaftliche Ergebnisse ohne Verzögerung zu verbreiten. Preprints können auf einem WWW-Server angeboten werden; am angenehmsten für den Leser ist es, wenn das gesamte Dokument im Hypertext-Format, auch mit Abbildungen, zur Verfügung gestellt wird. Hierfür gibt es von mir selbst, von Henry Rzepa und

anderen bereits Beispiele. Alternativ ist es aber auch möglich, nur das Abstract samt einem Verweis auf das PostScript-Dokument anzubieten; das Dokument kann dann ggf. vom Leser "heruntergeladen" werden. Selbstverständlich wirft diese Form des "Electronic Publishing" auch diverse Fragen auf, wie Copyright-Probleme, Authentizität der Dokumente, patentrechtliche Probleme und Gebührenerhebung."/KIR/

2.6.3 Sicherheit bei Gebrauch des Internet

Das Internet gilt als der größte Virenüberträger. Computerviren sind Programme die viel Schaden am Computer anrichten können (vgl. hierzu Kapitel 5). Hat man einen Virenscanner auf dem Rechner und setzt diesen auch ein, ist man schon relativ sicher. Dateien aus dem WWW oder Dateien, die an eine E-Mail gekoppelt sind, sollten auf jeden Fall überprüft, d.h. gescannt werden. Sobald man beginnt im Internet zu Surfen, sollte ein Virenscanner auf dem Rechner sein.

Eine sogenannte „Firewall" ist für den Privatanwender wohl unnötig. Für Betriebe o.ä. kann so eine Firewall notwendig und nützlich sein. Ein- und ausgehende Daten werden auf ihre Zulässigkeit überprüft und entweder durchgelassen oder gesperrt. Auch die Dienste im Internet, die ein Mitarbeiter nutzen kann, können reglementiert werden. Wichtig ist, dass derjenige, der von Außen auf die firmeneigenen Daten zugreifen will (und darf) trotzdem nicht direkt an die Daten kommt, sondern an eine Kopie dieser Daten auf einem extra dafür eingerichteten Server.

3 Ergonomie am Bildschirmarbeitsplatz

Als Fachkraft für Arbeitssicherheit (FaSi) wird man oft auch mit der Beurteilung von Bildschirmarbeitsplätzen beauftragt. Besonders in Branchen, bzw. Aufgabenfeldern, in denen viele Rechnerarbeitsplätze vorhanden sind, muss eine FaSi mit solch einer Aufgabenübertragung rechnen. Aber schon von ihren gesetzlichen Pflichten und Aufgaben her, ist es für eine FaSi notwendig, sich auch hier auszukennen.

Dass dieser Aufgabenbereich wichtig ist, kann man auch daran sehen, dass die Tätigkeit an Bildschirmarbeitsplätzen deutlich zugenommen hat. Man braucht nur an Versicherungen, Banken, Verwaltungen usw. denken. Mittlerweile arbeitet ca. jeder zweite Arbeitnehmer an einem Bildschirm und die Tendenz ist weiterhin steigend. /vgl. auch Poh, S. 1/

Im folgenden sollen einige, der Literatur entnommene Beispiele zeigen, dass die software- und hardwareergonomische Beurteilung der Computerarbeitsplätze eine wichtige Aufgabe ist; insbesondere für eine FaSi, deren Aufgabe es schließlich ist, gesundheitlichen Schaden des Arbeitnehmers zu verhindern. Denn bei Mitarbeitern, die an einem Bildschirm tätig sind, wurden verschiedene Beschwerden und krankhafte Störungen beobachtet:

Beispielsweise beschwerten sich bei einer Umfrage des Instituts für Arbeits- und Sozialforschung in Berlin ca. 57% der Befragen über Sehprobleme und Augenbrennen. In weiteren Forschungen war die Rede von Anstrengungs- und Ermüdungserscheinungen, Brennen und Jucken der Augen sowie vom Entstehen von Kurzsichtigkeit ebenso wie von Doppelsehen und Störungen des Farbempfindens. Weitere Ergebnisse waren, dass Mitarbeiter mit Tätigkeiten am Bildschirm häufiger über Kopfschmerzen klagen als andere Mitarbeiter (ca. 40% mehr). Auch Beschwerden des Muskel-Skelettsystems, vor allem im Bereich des Nackens (64% der Betroffenen, Doppelnennungen waren möglich), der Schultern (51%), des Rückens (40%) und der Arme (38%) wurden aufgenommen und als berechtigt anerkannt. Wieder andere Studien warnten vor der Möglichkeit einer Gesichtsdermatitis, die teilweise als Folgeerscheinung der Bildschirmarbeit entstehen könnte. Von einigen Seiten wurde über Schwangerschaftsstörungen berichtet, die bei einigen am Bildschirm tätigen Mitarbeitern auftraten. /Poh, S. 1; Men, S. 4; Schue, S. 21 ff./

Ein weiteres Phänomen, das im Zusammenhang mit Bildschirmarbeitsplätzen beobachtet werden kann, ist ein erhöhtes "Stress"-Empfinden. Dies steht in krassem Gegensatz zu dem Ziel \`Arbeitserleichterung´, wird aber häufig vom Arbeitgeber in Kauf genommen infolge der anderen Ziele \`Rationalisierung´ und \`Effektivvisierung´ der Arbeit. Durch dies erhöhte Stressempfinden werden jedoch oft die beiden letztgenannten Ziele nicht in gewünschtem Maße erreicht.

In diesem Zusammenhang werden grundsätzlich drei Stressfaktoren unterschieden:

⇒der Computer

Unzulängliches Hardware-Design, insbesondere minderwertige Bildschirme führen vor allem zur Überlastung des Auges. Schlecht gestaltete Tastaturen können zur Überlastung der Hände sowie der Arme führen. Eine schlecht gestaltete Software mit z.B. schlechtem Bild-Layout, schlechter oder wenig konstruktiver Hilfe und eine Anwendbarkeit, die viel Aufwand des Benutzers erfordert, führt zu deutlichen Stresserscheinungen. Der Zwang, sich der Computerlogik und/oder der Computersprache anzupassen sowie System-Response-Pausen, die eine gewisse, im normalen Geduldsrahmen liegende Antwortzeit überschreiten, und unvorhergesehene Unterbrechungen werden als Störung und Behinderung empfunden. /vgl. Men, S. 44 und 45/ Neuere Bildschirme und Tastaturen als auch Softwareprodukte sind ergonomisch deutlich besser; man glaubt aber nicht, wie viele alte `Schätzchen´ noch in Betrieb sind.

⇒die Arbeit

Zu hohe Anforderungen, z.B. durch Arbeitsintensivierung aber auch zu niedrige Anforderungen, z.B. durch Wegfall qualifizierter Tätigkeiten, führen in der Regel zu Stresserscheinungen. Eine ungenügend gestaltete Arbeitsumgebung, z.B. eine schlechte Einstellung des Arbeitsplatzes und/ oder die Belästigung durch Geräusche, falsche Beleuchtung und/oder unangemessene Lufttemperatur und -feuchtigkeit senken das Arbeitsniveau und das Arbeitsklima. Der durch die Einführung neuer Technologien und die regelmäßig erscheinenden Änderungen vorhandene Druck zur Weiterbildung, die häufig in der Freizeit anfällt, ist ebenfalls ein Stressfaktor, der nicht übersehen werden darf. /vgl. Men. S.45 bis 49/

⇒der (die) Mensch(en)

Dieser Stressfaktor an sich ist selbstverständlich nicht technologie-spezifisch. Technologiespezifisch können aber die auszulösenden Ängste sein. Dazu gehören z.B. die Angst davor, durch den Computer ersetzt zu werden. Auch die Angst, den Computerjargon nicht zu beherrschen oder den Computer durch falsche Anwendung (falschen Knopf drücken) zu beschädigen, ist technologiespezifisch. Hinzu kommen grundsätzliche Ängste wie z.B. vor Veränderungen, vor Gesundheitsschäden und vor der eigenen Blamage. /vgl. Men, S. 49 und 50/ Ganz allgemein kann beispielhaft als Stressfaktor noch festgehalten werden: Kollegen, mit denen man sich nicht versteht sowie Vorgesetzte, die einem unsympathisch sind und/ oder denen man unsympathisch ist.

3.1 Rechtsgrundlagen der Bildschirmarbeitsplätze

Die Auswirkungen durch Erkrankungen infolge mangelhafter ergonomischer Bildschirmarbeitsplätze betreffen zum einen den Menschen selbst (in seinem Wohlbefinden). Zum anderen belasten sie die Unternehmen und öffentlichen Arbeitgeber in Form von Kosten für Arbeitsausfälle und wirken sich gesellschaftlich in einer zusätzlichen Belastung des Gesundheitssystems aus. Daher wurden in der Bundesrepublik Deutschland schon frühzeitig Schutzbestimmungen gegen die Gefährdungen des Menschen bei Tätigkeiten an Bildschirmarbeitsplätzen entwickelt. Diese wurden zum Teil im Auftrag der Bundesregierung (ASR-Regeln) erstellt. Weiterhin gelten verschiedene Vorschriften der Berufsgenossenschaften (ZH-1-Schriften). Das Deutsche Institut für Normung (DIN) hat (unverbindliche) Richtlinien (Normen) aufgestellt.

3.1.1 Deutsche Vorschriften und Normen

Bei der Einrichtung und beim Betreiben von Bildschirmarbeitsplätzen müssen u.a. folgende Vorschriften verbindlich berücksichtigt werden:

⇒Bildschirmarbeitsverordnung vom 4. Dezember 1996

⇒Sicherheitsregeln für Bildschirmarbeitsplätze im Bürobereich ZH 1/618 von Oktober 1980

⇒Sicherheitsregeln für Büroarbeitsplätze ZH 1/535 von Januar 1976

⇒Arbeitstättenverordnung:

- ◊ § 5 - Lüftung, dazu Arbeitsstättenrichtlinie 5 (ASR 5)
- ◊ § 6 - Raumtemperatur (dazu ASR 6/1,3)
- ◊ § 7 - Beleuchtung (dazu ASR 7/3 und 7/4)
- ◊ § 8 - Fußböden (dazu ASR 8/1)
- ◊ § 9 - Fenster und Oberlichter (dazu ASR 7/1 und 8/4)
- ◊ § 10 - Türen und Tore (dazu ASR 10/1 und 10/5)
- ◊ § 15 - Schutz gegen Lärm
- ◊ § 23 - Raumabmessungen / Luftraum
- ◊ § 24 - Bewegungsfläche am Arbeitsplatz

Diese Vorschriften können bei den Berufsgenossenschaften angefordert werden oder direkt beim Carl Heymanns Verlag /CHV/ bezogen werden.

Daneben existieren eine Vielzahl von Normen, deren Beachtung jedoch nicht rechtsverbindlich vorgeschrieben ist. Sie gelten jedoch als Stand der Technik und sollten deshalb beachtet werden. Normen können über den Beuth-Verlag /Beu/ bezogen werden. Die CD-ROM `PERINORM´ enthält ein Normenverzeichnis, mit dessen Hilfe entsprechende Normen herausgefiltert werden können. Beispielhaft genannt werden hier:

⇒DIN 2137 ff. Tastaturen
⇒DIN 21 48 Tastaturen, Begriffe
⇒DIN 33 400 Gestaltung von Arbeitssystemen nach arbeitswissenschaftlichen Erkenntnissen
⇒DIN 66 233 f Bildschirmarbeitsplätze, Begriffe
⇒DIN 66270 ff. Bewerten von Software (-dokumenten, -produkten, -fehler usw.)

3.1.2 Europäisches Recht

Unter Berufung auf den EU-Vertrag, Artikel 118a, wurde am 12. Juni 1989 die \`Richtlinie über die Durchführung von Maßnahmen zur Verbesserung der Sicherheit und Gesundheitsschutzes der Arbeitnehmer bei der Arbeit´ (Richtlinie 89/391/EWG) erlassen. Im Rahmen dieser Arbeitsschutz-Richtlinie wurden, gestützt auf Abschnitt IV - Artikel 16, weitere Richtlinien erlassen, u.a. die Richtlinie 90/270/EWG: \`Richtlinie des Rates vom 29. Mai 1990 über die Mindestvorschriften bezüglich der Sicherheit und des Gesundheitsschutzes bei der Arbeit an Bildschirmgeräten (5. Einzelrichtlinie im Sinne von Artikel 16, Absatz 1 der Richtlinie 89/391/EWG).´ Diese Richtlinien begründen einen Rechtsanspruch, auf den sich ein Mitarbeiter berufen kann, wenn er auf Einhaltung der Vorschriften besteht. Dieser Anspruch ist gegebenenfalls einklagbar. Dass dies nicht nur Theorie ist, zeigt folgendes Urteil des Bundesarbeitsgerichtes:
“Pausen bei Bildschirmarbeit
Der Betriebsrat kann durchsetzen, dass Bildschirmarbeit durch regelmäßige Pausen oder andere Tätigkeiten unterbrochen wird. Allerdings kann er nicht fordern, dass der Arbeitgeber kostenlose Augenuntersuchungen anbietet. (Bundesarbeitsgericht, 1 ABR 47/95)
Damit lehnt sich das Bundesarbeitsgericht an die EG-Bildschirmrichtlinie von 1990 an.” /FOCUS Online GmbH, 1996/
Diese Richtlinien hätten zum 31. Dezember 1992 in Deutsches Recht umgesetzt sein müssen. Im Herbst 1996 trat dann endlich die lang erwartete Bildschirmarbeitsverordnung in Kraft. /vgl. auch Poh/

3.1.3 Bildschirmarbeits-Verordnung

Die Bildschirmarbeitsverordnung ist ein Teil des ebenfalls 1996 verabschiedeten Arbeitsschutzgesetzes (Bezug auf § 19 des Arbeitsschutzgesetzes vom 7. August 1996) und konkretisiert dessen Bestimmungen bezüglich von Bildschirmarbeitsplätzen. Der Wortlaut der Verordnung, Anmerkungen zum Geltungsbereich und zur Pausenregelung können im Anhang (Anhang 3-1 bis 3-4)

nachgelesen werden. Die Bildschirmarbeits-Verordnung umfasst im wesentlichen folgende gesetzliche Regelungen:

⇒Bildschirmarbeitsplätze müssen der Verordnung und den sonst geltenden Arbeitsschutz- und Unfallverhütungsvorschriften entsprechen; d.h. bestimmte Mindestanforderungen müssen erfüllt sein.

⇒Um Behinderten die Arbeit an Bildschirmarbeitsplätzen zu ermöglichen, können diese unter Berücksichtigung der Belange und Fähigkeiten der Betroffenen von den oben angegebenen Regeln abweichen.

⇒Eine Arbeitsplatzanalyse ist durchzuführen.

⇒Arbeitsablauf und Pausen müssen so gestaltet sein, dass durch andere Tätigkeiten oder Pausen die Arbeitszeit am Bildschirm eine angemessene Dauer nicht überschreitet. Vorgeschlagen werden daher eine Mischtätigkeit; wenn dies nicht durchführbar ist, häufigere kleine Pausen einplanen.

⇒Augen und Sehvermögen der Mitarbeiter müssen untersucht werden.

⇒Es besteht eine Unterrichtungs- und Unterweisungspflicht des Arbeitgebers. Dies wird in der Regel als Schulungspflicht interpretiert. Auch das Gewähren von Zeit zum Kennenlernen und Vertrautmachen mit der Hard- und Software, den Hilfsmitteln und der sonstigen Büroeinrichtung gehört dazu.

⇒Sanktionen (Bußgelder, Freiheitsstrafen) bei Nichtbeachten der Verordnung werden angedroht.

Bildschirmarbeitsplatzanalysen können von internen Mitarbeitern durchgeführt werden, sofern sie über die erforderliche Sachkunde verfügen. Sofern eine Fachkraft für Arbeitssicherheit nicht ohnehin schon mit der Beurteilung der Bildschirmarbeitsplätze betraut war, spätestens seit in Kraft treten dieser Verordnung muss sie sich mit diesem Thema befassen. Denn die Arbeitssituation am Bildschirm muss als Ganzes gesehen werden. Nicht nur Hardware und Büromöbel werden begutachtet, sondern auch Software-ergonomie und Arbeitsorganisation und die daraus abzuleitende psychische Belastung des am Bildschirm Tätigen.

3.2 Die Beurteilung von Bildschirmen

Der Mensch nimmt Informationen in erster Linie mit Auge und Ohr auf. Dazu kommen die Möglichkeit über Tastsinn, Geschmacksinn, Riechsinn und Temperatursinn weitere Informationen wahrzunehmen. Solche Wahrnehmungen, Informationsaufnahmen lösen unspezifische Empfindungen aus, die z.B. Zuwendung (positive Empfindung) oder Ablehnung (negative Empfindung) beinhalten können. Beispielsweise kann Musik einerseits als beruhigend aber andererseits als Krach, d.h. als störend und nervend empfunden werden. Auch Wärme kann eine wohltuende Empfindung auslösen oder im Gegensatz dazu lästig und unangenehm wirken. Ebenso werden mit

Farben Empfindungen verknüpft; rot wird in der Regel als warm und angenehm gesehen, blau wird hingegen als kühl, oft als kalt empfunden. /vgl. Kru/
Bei der Arbeit an Bildschirmarbeitsplätzen bedarf es in erster Linie der visuellen Wahrnehmung. Um diese visuelle Wahrnehmung zu ermöglichen, verfügt der Mensch im allgemeinen über:

⇒den *`optischen Apparat´;*
dies ist die Augenoptik, mit der ein Bild der Umwelt auf die lichtempfindliche Netzhaut geworfen wird.

⇒die *`Augenmotorik´;*
sie dient der Einstellung der Sehentfernung (Akkommodation) und der Ausrichtung der Augenachsen.

⇒das *`visuelle Nervensystem´,*
Überleitung zum und Verarbeitung des Bildes im Großhirn.

Das Hauptkennzeichen für die Leistungsfähigkeit des Auges ist die Sehschärfe. Die Sehschärfe beim Menschen hängt ab von der:

⇒*Netzhautart;*
⇒*Akkommodationsfähigkeit* (Sehschärfe einstellen);
⇒*Adaptionszustand* (Adaption ist Helligkeitsanpassung);
⇒*Alter* (mit steigendem Alter in der Regel nachlassende Sehleistung).

Die Sehschärfe hängt aber auch vom wahrzunehmenden Objekt ab. Von Bedeutung ist der Bewegungszustand des Objektes; in Ruhe befindliche Objekte können besser fixiert werden aber sich bewegende Objekte werden in der Regel besser wahrgenommen. Der Kontrast, die Farbe und die Leuchtdichte eines Objektes sind ebenfalls wesentliche Faktoren, die einen großen Einfluss auf die Sehschärfe haben.
Berücksichtigt man dieses Wissen, ergeben sich Kriterien wie Anzeigeart, Zeichengröße, Zeichenschärfe, Kontrast, Farbmöglichkeiten etc. nach denen der Bildschirm beurteilt und ausgewählt werden kann. Die im folgenden dargestellten Erkenntnisse und Empfehlungen wurden übernommen aus einer amtlichen Studie des Bayrischen Staatsministeriums für Arbeit und Sozialordnung, erstellt von Prof. H. Krueger /Kru/. Obwohl die vorliegende Ausgabe von 1989 ist, konnte der wesentliche Inhalt direkt übernommen werden, denn auch neuere Literatur /vgl. z.B. Schue/ weicht nur unwesentlich von der zitierten Quelle ab.

3.2.1 Art der Anzeige

Prinzipiell können zwei Arten der Darstellung der Zeichen angewendet werden. Die mittlerweile übliche Anzeigeart sind dunkle Zeichen auf hellem Grund. Hier spricht man von positiver Polarität. In den Anfangszeiten der EDV war die

Darstellungsart in der Regel helle Zeichen auf dunklem Grund (negative Polarität). Man spricht nunmehr auch von Inversdarstellung (vgl. Bild 3-1).

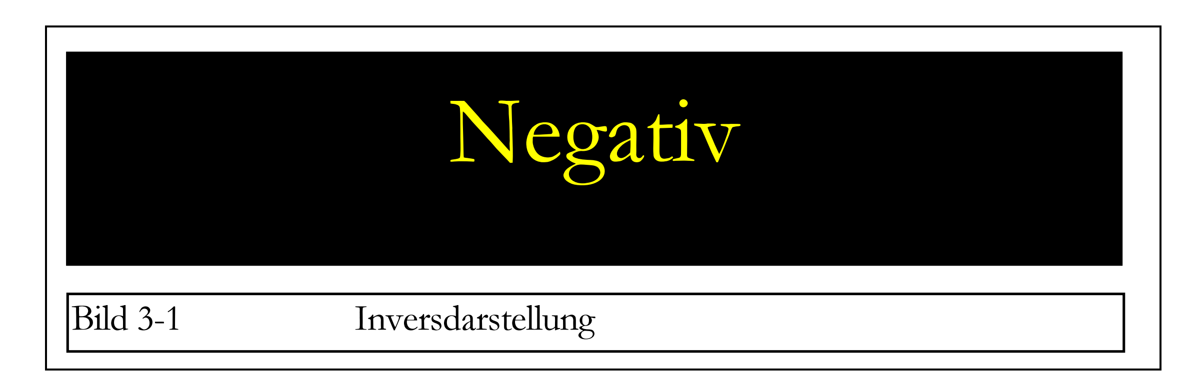


Bild 3-1 Inversdarstellung

Anmerkung: Die Leuchtdichteangaben bei der Beschreibung eines Bildschirms beziehen sich bei positiver Polarität auf den Hintergrund, bei Inversdarstellung auf die Zeichen selbst.

3.2.2 Zeichengröße

Nur in einem Bereich von cirka 10 bis 20 Sehwinkelminuten Durchmesser kann man wirklich scharf sehen. Um flüssig lesen zu können, müssen cirka 4 bis 6 Buchstaben sicher erkannt werden sowie ungefähr 15 bis 20 Buchstaben im Umriss der Worte gesehen werden. Daraus folgt, dass die Buchstaben nicht zu klein sein dürfen, aber auch nicht zu groß. Für die Zeichengröße sollte daher folgende Bedingung erfüllt sein:

$$0{,}052 * e < \text{Zeichengröße [mm]} < 0{,}07 * e \qquad e = \text{Sehentfernung [cm]}$$

“Empfehlung:
Bezogen auf einen minimalen akzeptablen Wert der Sehentfernung von 50 cm soll die Zeichenhöhe zwischen 2,6 und 3,6 mm betragen. Für größere Sehentfernungen muss die Zeichengröße entsprechend linear vergrößert werden. Da die Sehentfernung von 50 cm auf Dauer nicht unterschritten wird (Zurücklehnen beachten) und es Personen mit reduzierter Sehschärfe gibt, soll die Höhe des Zeichens 2,6 mm nicht unterschreiten. In Spezialfällen, wenn z.B. bei graphischen Bildschirmen oder bei der Gestaltung ganzer Textseiten (DIN A4) nicht die Information des einzelnen Zeichens im Vordergrund steht, kann die minimale Höhe unterschritten werden.” /Kru, S. 14/

3.2.3 Zeichenschärfe

Bei der Zeichenschärfe ist zu beachten, dass scharfe Zeichen besser wahrgenommen werden als unscharfe Zeichen. Denn unscharfe Zeichen geben der Akkommodation einen geringeren Anreiz als scharfe Zeichen. Daraus folgt

eine zusätzliche funktionelle Unschärfe. Die Zeichenschärfe scheint bei monochromen Bildschirmen höher als bei Farbschirmen zu sein. Daher kann man für reine Textverarbeitung einen monochromen Bildschirm empfehlen. In der Regel ist die Zeichenschärfe im Zentrum des Bildschirms besser als am Rand. Bei positiver Polarität des Bildschirms hat man den Eindruck, dass die Zeichenschärfe besser ist als bei negativer Polarität (vgl. Bild 3-2). Mit der Leuchtdichte ändert sich die Zeichenschärfe, ab dem Maximum an Schärfe gilt: Je höher die Leuchtdichte desto schlechter die Zeichenschärfe.

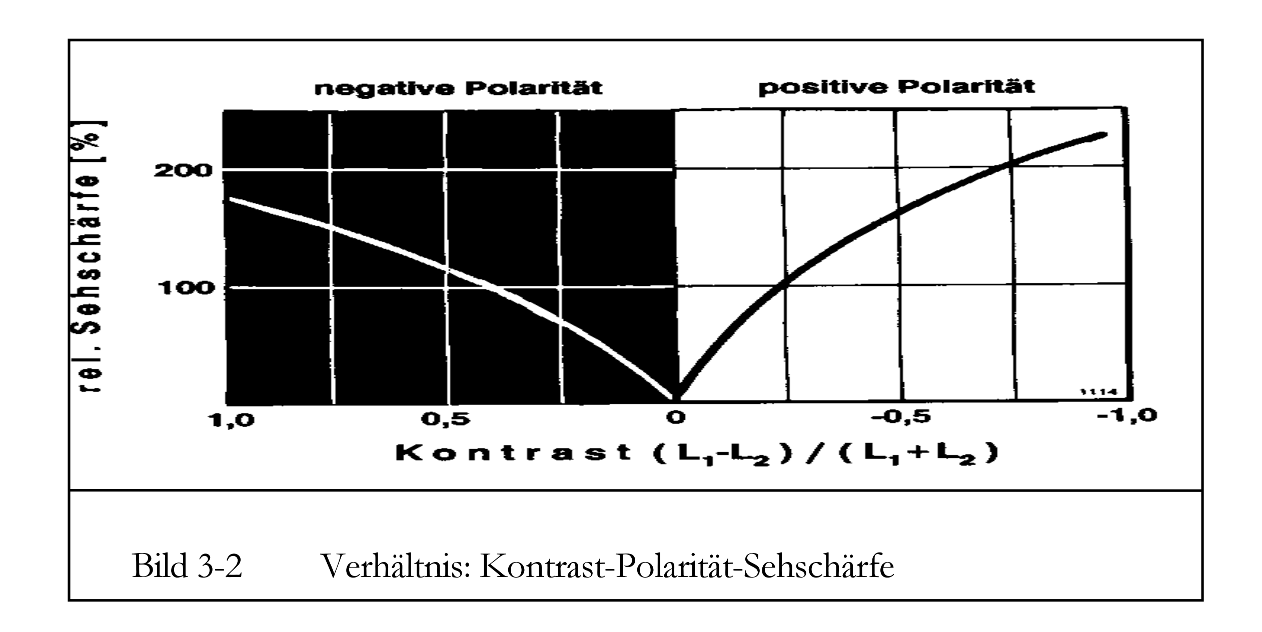


Bild 3-2 Verhältnis: Kontrast-Polarität-Sehschärfe

“Empfehlung:
Es sind Bildschirme mit Zeichen zu wählen, deren Schärfe derjenigen von gedruckten Zeichen möglichst nahe kommt.
...
Die Zeichenschärfe wird in den Randbereichen des Bildschirms beurteilt.” /Kru, S. 15/

3.2.4 Zeichenleuchtdichte

Bei positiver Polarität bestimmt der Hintergrund die Leuchtdichte, während bei negativer Polarität das Zeichen die Leuchtdichte bestimmt. Es ist zu beachten, dass hellere Räume einen helleren Bildschirm erfordern. Die Kontraste in einem größeren Feld dürfen nicht allzu groß sein. Um ein angenehmes Arbeiten zu ermöglichen, muss die mittlere Leuchtdichte hinreichend groß sein (~ 150 cd/cm^2 gilt als gut). Die Blendwirkung der (hellen) Umwelt steigt bei fallender Untergrundleuchtdichte.

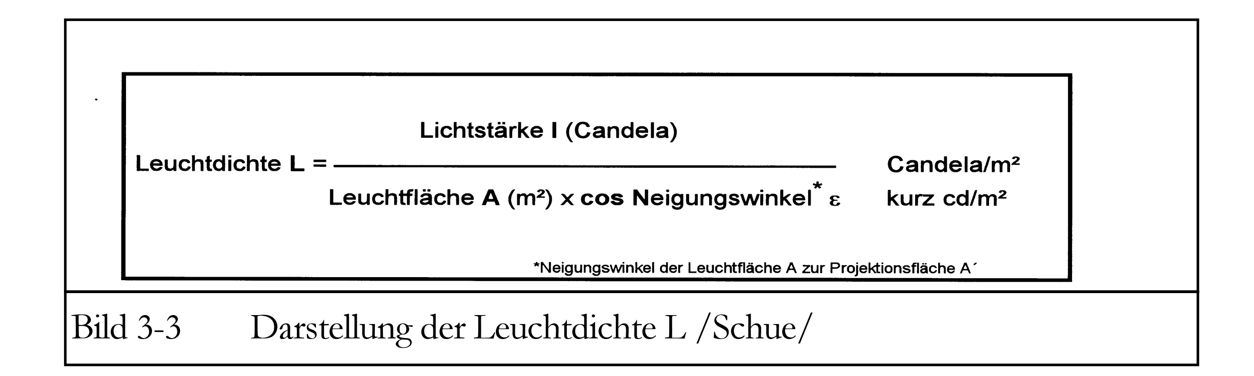


Bild 3-3 Darstellung der Leuchtdichte L /Schue/

“Empfehlung:
Die Zeichenleuchtdichte selbstleuchtender Bildschirme sollte für Räume mit üblicher Beleuchtung und Einrichtung einen Wert von wenigstens 160 cd/cm^2 erreichen. Die Angabe einer oberen Grenze erübrigt sich. Die Leuchtdichte auf dem Bildschirm (Zeichen bzw. Untergrund) soll den Bedürfnissen des Benutzers und den Erfordernissen der allgemeinen Raumhelligkeit entsprechend individuell angepasst werden können.” /Kru, S. 16/

3.2.5 Zeichenkontrast

Bei zu geringen Kontrasten (K < 1:3 bzw. 3:1) ist das Erkennen bezüglich Wahrnehmungsgüte als auch Wahrnehmungsgeschwindigkeit gestört. Bei positiver Polarität existiert keine Grenze nach oben; bei negativer Polarität liegt der Grenzwert des Kontrastes bei ca. 1:20, denn zu helle Zeichen auf zu dunklem Grund blenden.

“Empfehlungen:
Die unterste Grenze des äußeren Kontrastes beträgt 1:3 bzw. 3:1. Für helle Zeichen auf dunklem Grund ist zudem eine obere Grenze von etwa 1:20 einzuhalten.
Optimale Zeichenkontraste liegen zwischen 1:6 und 1:10 (negative Polarität) bzw. über 6:1 (positive Polarität).” /Kru, S. 17/

3.2.6 Zeichenfarbe

Die Farben eines Farbbildschirms werden durch Mischen von Rot, Grün und Blau erzeugt. Sie unterscheiden sich von natürlichen Farben durch eine größere Sättigung (und damit in ihrer spektralen Zusammensetzung). Ungesättigte Farben haben eine breite spektrale Energieverteilung, dagegen bestehen gesättigte Farben im idealen Fall aus einer Spektrallinie.
Reiner Farbkontrast ohne Leuchtdichteunterschied wird als unangenehm empfunden. Das menschliche Auge hat eine unterschiedliche spektrale Empfindlichkeit, d.h. für verschiedene Wellenlängen des sichtbaren Lichtes

werden unterschiedliche Energien für die gleiche Wirkung benötigt. Die größte Empfindlichkeit des Auges liegt bei Grün (550 nm).

"Empfehlungen:
Bei monochromen Bildschirmen bewähren sich Unbunt (weiß) sowie grüne bis gelborange Farben mit möglichst breiter spektraler Energieverteilung. ... Die Vorteile von Farben kommen vor allem beim Kodieren graphischer Informationen zur Geltung. Bei reiner Textverarbeitung sind monochrome Bildschirme zu bevorzugen.
Der Einsatz von Farbe ist sorgfältig zu planen (Farbwahl, Farbfehlsichtigkeit).
Reine Farbkontraste sind zugunsten von Hell-Dunkel-Kontrasten zu vermeiden. ..." /Kru, S. 18/

3.2.7 Zeichengestalt

Um ein gutes Lesen zu ermöglichen, muss eine gewisse Strichstärke da sein. Diagonale Linien sollen nicht gestuft sein. Die Zeichenleuchtdichte sollte in jeder Richtung konstant sein. Die Buchstaben sollen deutlich erkennbare Ober- und Unterlängen haben (wie in Bild 3-4 dargestellt) und die Zeichengestalt sollte dem vom Papier gewohntem Bild entsprechen.
Die Fehlersuche in Texten gelingt auf Papier besser als am Bildschirm. In der Regel achtet man auf Wortanfang und Wortende, d.h. die meisten Tippfehler, Verdreher etc. sind der Wortmitte.

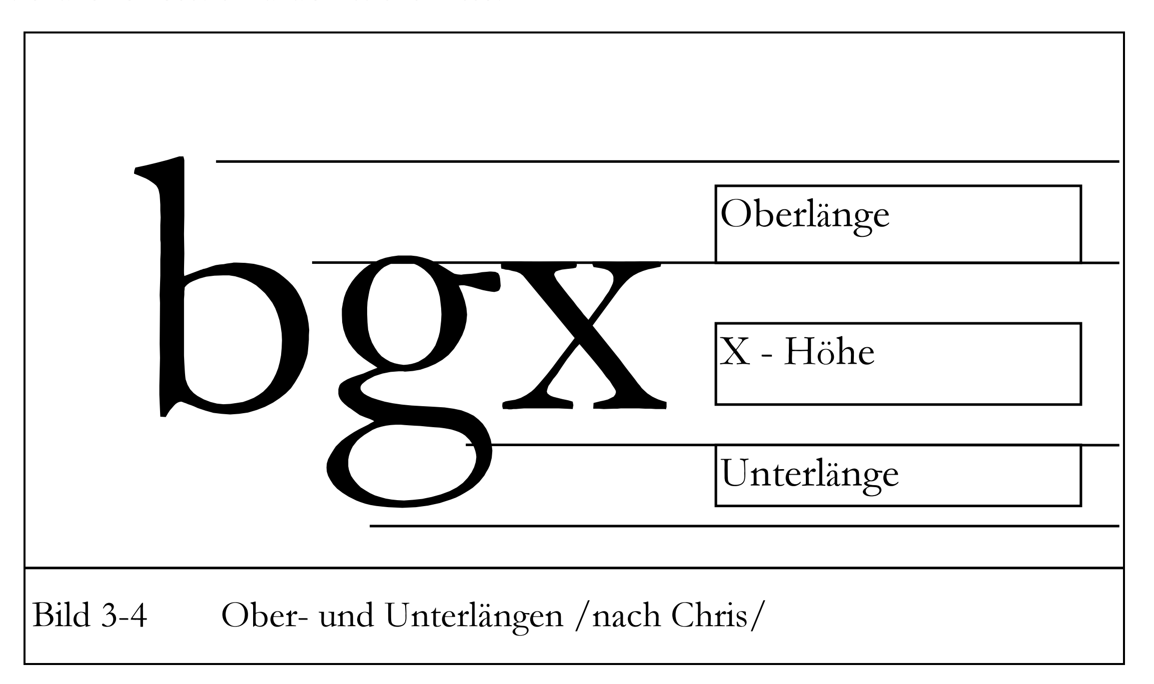


Bild 3-4 Ober- und Unterlängen /nach Chris/

"Empfehlungen:
Es soll ein Zeichensatz gewählt werden, der dem gewohnten Erscheinungsbild gleicht. Große und kleine Buchstaben unterstützen als Strukturmerkmal ein schnelles Auffinden von Informationen. Auf eine deutlich wiedererkennbare äußere Form der Wörter ist Wert zu legen (Ganzwortlesen)." /Kru, S. 19/

3.2.8 Zeichenstabilität

Zitterbewegungen (werden als Jitter bezeichnet) der Zeichen mindern die Zeichenschärfe; sie stören die Fixation der Zeichen und ab. Jitter sind im peripheren Sehfeld eher wahrzunehmen als im zentralen Sehfeld. Bei neueren Monitoren ist dies normalerweise eine unbekannte Erscheinung, es sei denn äußere Magnetfelder beeinflussen den Bildschirm.
"Empfehlungen:
Gute Bildschirme weisen praktisch kein `Jitter´ auf. Bewegt sich das Bild dennoch, sind in der Regel äußere Magnetfelder (Lüftermotoren, Lautsprecher, sonstige elektrische Geräte) die Ursache, die es zu beseitigen gilt." /Kru, S. 19/

3.2.9 Zeilenabstand

Häufig fällt es schwer, vom Ende einer Zeile ausgehend zum Anfang der nächsten Zeile zu finden. Dies tritt bei unstrukturierten Texten auf. Auch einzeilige oder noch geringere Zeilenabstände erschweren diesen Wechsel. Besonders problematisch ist dies, wenn bei der Arbeit am Rechner dauernd zwischen Beleg und Bildschirm gewechselt werden muss. Die Arbeit erleichtern kann ein größerer Zeilenabstand, der folgende Bedingung erfüllt:

$(d-z)/l > 0{,}05$
(d : Zeilenabstand in mm, z : Zeichengröße in mm, l : Zeilenlänge in mm)

"Empfehlung:
Ein ausreichender Zeilenabstand ist besonders bei Korrekturaufgaben am Bildschirm einzuhalten. Für die Fehlersuche in Texten ist nur 1,5 bis 2 zeilige Schreibweise geeignet. Längere Zeilen erfordern einen größeren Zeilenabstand als kurze." /Kru, S. 20/

3.2.10 Flimmern

Die Leuchtdichte der Punkte des Bildschirms oszilliert. Oberhalb der Flimmerverschmelzungsfrequenz (FVF) wird diese Oszillation vom Auge nicht mehr registriert; es wird eine konstante Helligkeit wahrgenommen. Diese Frequenz hat keinen festen Wert, u.a. da sie im seitlichen Gesichtsfeld größer als im zentralen Gesichtsfeld ist. Die Flimmerverschmelzungs- frequenz (FVF) ist beeinflusst von:

⇒der mittleren Leuchtdichte (Sie steigt mit zunehmender Leuchtdichte); d.h. Bildschirme mit positiver Polarität haben in der Regel eine höhere Flimmerverschmelzungsfrequenz.
⇒zeitlicher Verlauf der Leuchtdichte (Oszillation)
⇒Größe des flimmernden Feldes (große Felder haben höhere FVF)
⇒Ort des flimmernden Feldes im Gesichtsfeld (im Zentrum ist FVF am kleinsten)
⇒Sehschärfe (je geringer die Sehschärfe desto geringer die FVF)
⇒Alter und zentralnervöse Ermüdung (FVF sinkt)
⇒Augenbewegungen (Bei häufigem Wechsel der Blickrichtung)
⇒die FVF kann bei über 90 HZ liegen.

“Empfehlung:
Flimmern ist auf jeden Fall zu vermeiden, da Flimmern die Aufmerksamkeit erregt und von der Arbeit ablenkt. Es ist ein für die Aufgabe tolerabler Phosphor langer Nachleuchtdauer zu wählen (kleiner Oszillationsgrad). Erst oberhalb einer Nachleuchtdauer von 10 ms kann von langsamen Phosphoren gesprochen werden. Bei positiver Polarität wird eine höhere Frequenz benötigt als bei negativer Polarität.
Eine gesamthafte Aufhellung der Bildschirmoberfläche durch an der Bildschirmoberfläche reflektiertes Raumlicht senkt die wirksame Oszillation des Bildschirms und führt damit zu einer kleiner FVF.” /Kru, S. 21/

3.2.11 Zeichenpolarität

Herkömmlich werden Texte auf hellem Untergrund (Papier) mit schwarzen Zeichen dargestellt. Untersuchungen haben gezeigt, dass die Sehschärfe für Zeichen positiver Polarität besser ist. Insbesondere beim Wechsel Beleg zu Bildschirm und zurück erweist sich die Darstellung in positiver Polarität als augenfreundlicher. Daher hat sich die Darstellung in positiver Polarität bei Bildschirmen durchgesetzt. Die Inversdarstellung wird nur noch in Ausnahmefällen benutzt.

Positive Zeichenpolarität

Negative Zeichenpolarität (Inversdarstellung)

Bild 3-5 Zeichenpolarität

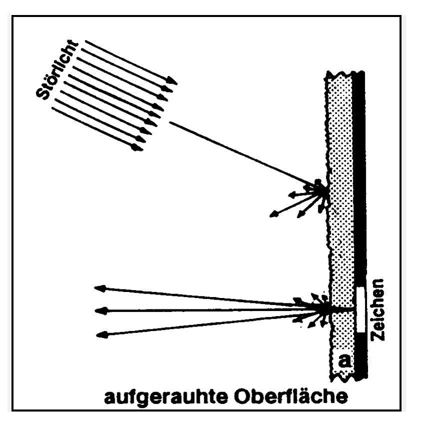
Empfehlung:
Grundsätzlich ist die positive Polarität (dunkle Zeichen auf hellem Grund) zu verwenden. Der Gebrauch der negativen Polarität bedarf besonderer Gründe. /vgl. Kru, S. 22/

3.2.12 Reflexe

Bildschirme haben eine Oberfläche aus optisch durchsichtigem Material. Dies hat die Eigenschaft, einen Teil des auf die Oberfläche treffenden Lichtes zu reflektieren. Lichtreflexe erschweren die Arbeit mit dem Bildschirm. Oft bemüht sich der Benutzer durch (leider ungeeignete) Maßnahmen wie Anpassung der Körperhaltung die negativen Auswirkungen zu vermeiden. Es gibt verschiedene Methoden des Reflexschutzes:

⇒positive Polarität ist erster Reflexschutz

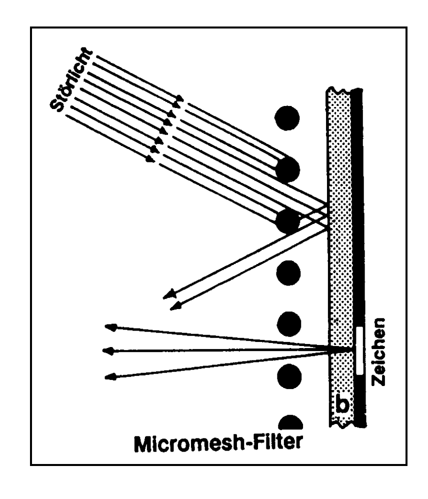
⇒aufgeraute Oberfläche (gerichtete Reflexe werden zu diffusen)



◊ geringere Leuchtdichte der Reflexe
◊ Unschärfe der Reflexe -> kein Anreiz fürs Auge
◊ `Verschleierung´ der Zeichen (negativer Aspekt)

Bild 3-6 aufgeraute Oberfläche /Kru/

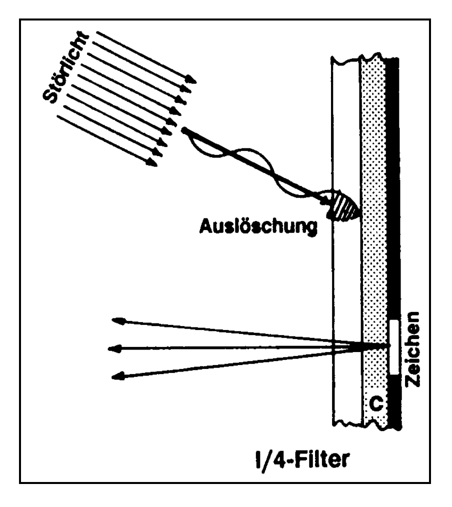
⇒Mikromesh-Filter



◊ feines mattschwarzes Gitter als Vorsatz
◊ Bildschirmhintergrund erscheint tiefschwarz -> sehr hohe Kontraste
◊ sind mechanisch sehr empfindlich; verstauben leicht

Bild 3-7 Mikromesh-Filter /Kru/

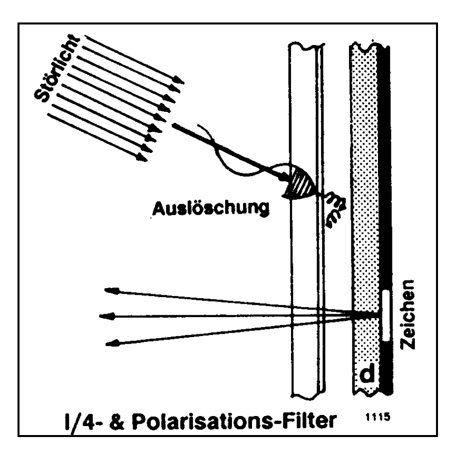
⇒Oberflächenvergütung



◊ entspricht der Vergütung bei Photoobjektiven (teuer!)
◊ ändert die Schärfe der Zeichen nicht
◊ Transmission für das Licht der Bildpunkte wird beeinflusst

Bild 3-8 l/4 Schicht /Kru/

⇒Polarisationsfilter



◊ zusätzlich zur Oberflächenvergütung
◊ polarisieren das von den Bildschirmpunkten ausgehende Licht
◊ die Leuchtdichte (der Bildpunkte) wird halbiert

Bild 3-9 l/4 Schicht & Polarisationsfilter /Kru/

“Empfehlung:
Grundsätzlich sollte ein Bildschirm mit optischer Vergütung gewählt werden. Alle anderen Reflexschutzmaßnahmen bedürfen einer speziellen Begründung.
Bildschirme mit geringer Oberflächenkrümmung (großer Krümmungsradius) lassen sich leichter reflexfrei aufstellen als solche mit stark gekrümmter Oberfläche.
Reflexschutzmaßnahmen sind nur bei regelmäßiger Wartung wirksam.” /Kru, S. 24/

3.2.13 Eigenleistung der Arbeitnehmer

Bei der Arbeit an dem Bildschirm hat der Arbeitnehmer einige Möglichkeiten, sich die Arbeit zu vereinfachen (oder auch zu erschweren), wenn er die folgenden Ratschläge von H.Krueger beachtet (oder nicht beachtet):

"**Augenermüdung**

Langandauernde Naharbeit bedeutet für den Akkommodationsmuskel (Ziliarmuskel) ermüdende Haltearbeit. Er sollte deshalb regelmäßig entlastet werden. Dieses geschieht am besten durch einen Wechsel der Sehentfernung zwischen nah und fern. Auch sollte der Benutzer eines Bildschirms nicht vergessen, dass er für die Einstellung guter Sehbedingungen mitverantwortlich ist.

Brillen

Getönte Bildschirmbrillen sind im allgemeinen für den Arbeitsplatz mit Bildschirm ungeeignet. Ältere Arbeitnehmer mit eingeschränkter Möglichkeit, das Auge auf verschiedene Entfernungen scharf einzustellen, benötigen eine Altersbrille zur Anpassung des Auges an unterschiedliche Sehentfernungen. Altersbrillen sind jeweils ein Kompromiss an die erforderlichen Sehdistanzen. Sie müssen den Sehanforderungen am individuellen Arbeitsplatz angepasst werden. Altersichtige Personen können die Arbeit des Arztes oder des Optikers unterstützen, wenn sie die kürzeste, die größte und häufigste Sehentfernung an ihrem speziellen Arbeitsplatz messen. Weiterhin ist es wichtig, sich einen Überblick über die zeitliche Folge der Sehentfernungen bei verschiedenen Arbeiten (Bildschirm, Beleg, Kundengespräch, Personalbetreuung) zu verschaffen. Eine Strichliste kann dazu nützlich sein. Bei vorwiegender Arbeit am Bildschirm sind monofokale Gläser (Einstärkengläser) vorzuziehen. Bifokale Brillen sollten im zentralen Teil des Brillenglases auf die Entfernung des Bildschirms abgestimmt sein. Das Tragen einer Brille, die in das Wirkungsgefüge der Entfernungseinstellung mit `Akkommodation-Fusion-Pupillenweite´ eingreift, will gelernt und ständig geübt sein! Neue Brillen werden deshalb zuerst als störend empfunden. Daher sollten die Brillen auch getragen werden. Staubpartikel und Fingerabdrücke auf den Brillengläsern wirken als Blendquellen. Ungeputzte Brillen erschweren besonders bei blendempfindlichen älteren Personen die Wahrnehmung. Eine Brille kann ihre Wirkung deshalb nur dann entfalten, wenn sie ständig getragen und regelmäßig geputzt wird.

Wartung der Bildschirmoberfläche

Verschiedene Faktoren, die in den Verantwortungsbereich des Benutzers fallen, erschweren die visuelle Wahrnehmung. Bildschirmoberflächen laden sich im Betrieb elektrostatisch auf. Dadurch verstauben sie schneller. Bei vorgesetzten

Filtern kann auch der Raum zwischen Filter und Bildschirmoberfläche verstauben. Im regelmäßigen Gebrauch sinken deshalb Schärfe und Kontrast der Zeichen. Folglich ist eine regelmäßige Wartung der Bildschirmoberfläche notwendig. Der Reflexschutz, sei es eine physikalische Entspiegelung, eine aufgeraute Oberfläche oder auch ein Mikromesh-Filter, wird durch den Schweiß eines suchenden Fingers, der zur Erleichterung der Augenbewegungen über den Bildschirm geführt wird, lokal aufgehoben und herabgesetzt. Unbeabsichtigt entstehen so zahlreiche entspiegelte Flecken auf dem Bildschirm. Deshalb: Keine Fingerabdrücke und regelmäßige Reinigung nach Angaben des Herstellers.

Beleuchtung
Zu starke Abdunkelung des Arbeitsraumes mindert die Lesbarkeit von Belegen, ohne die Arbeit am Bildschirm wesentlich zu verbessern. Zusätzliche farbige Vorhänge stören die Farbadaption und die visuelle Wahrnehmung.

Kleidung
Auffällige Kleidung (z.B. weiße Kleidung oder solche mit starken Kontrasten) kann im Bildschirm störend spiegeln. Die Aufmerksamkeit wird abgelenkt und die Einstellung der Sehentfernung gestört." /Kru, S.61/62/

3.3 Beurteilung der sonstigen Hardware, Empfehlungen
Unter ergonomischen Gesichtspunkten sind noch die Eingabegeräte (Tastatur, Maus etc.) sowie weitere Ausgabegeräte wie Drucker, Plotter und Ausgabegeräte zu beachten.

3.3.1 Weitere Ausgabegeräte
Für Drucker und Plotter gelten - von bildschirmspezifischen Erkenntnissen zu Jitter, Flimmern und Reflexen abgesehen - die gleichen ergonomischen Prinzipien für Schriftsatz, -bild etc. Daher sind an "Zeichen und Schriftqualität dieselben Anforderungen zu stellen wie beim Bildschirm. Es soll ein leiser Drucker gewählt werden, da Schallschutz an der Quelle billiger ist." /Kru, S. 24/
Akustische Informationsausgabe kann von Interesse sein bei Überlastung des Auges oder kann nützlich sein für die Lenkung der Aufmerksamkeit außerhalb des zentralen Gesichtsfeldes. Der allgemeine Geräuschpegel am Arbeitsplatz

> Ein Kunde beschwerte sich über einen Monitor, bei dem man keinen Kontrast mehr regeln könnte. Ich vor Ort und sehe mir das Ding an. Festgestellt, dass der Monitor einen Bildschirmfilter hat, der nicht fest draufsitzt. Also den Filter abgezogen und den Monitor betrachtet, auf dem sich eine fossile Staubschicht der letzten Jahre breitgemacht hatte...
> Soviel zum Thema Kontrast.
> From: Maja Hulicka, maja.hulicka@zx.x400.basf-ag.de

sollte um wenigstens 10 dB(A) überschritten werden. Für unbekannte Informationen setzt Krüger eine Lautstärke von 20 dB(A) über dem Geräuschpegel am Arbeitsplatz an.
Eine akustische Informationsausgabe hat den Vorteil, dass Sehbehinderten die Arbeit mit dem Computer ermöglicht wird. Die Sprachausgabe ist mittlerweile soweit fortgeschritten, dass sich Sehbehinderte einen Text fließend vorlesen oder für die Fehlerkorrektur buchstabieren lassen können.

3.3.2 Eingabegeräte, speziell Tastatur

Die Tastatur ist immer noch das wesentliche Hilfsmittel bei der Arbeit am Rechner, insbesondere bei der Dateneingabe - trotz Scanner, Graphiktableau, Maus usw. Eine ergonomische Auslegung der Tastatur beeinflusst den Arbeitserfolg wesentlich. Bei der Beurteilung und Auswahl einer Tastatur sollte die DIN 2148 beachtet werden. Krüger hat in Anlehnung an die DIN und darüber hinaus folgende Ratschläge formuliert:
1. zur Tastengestaltung:
- ◊ "Allein konkave Tastenoberflächen bieten eine gute seitliche Fingerführung.
- ◊ Größe und Abstand der Tasten müssen anthropometrisch richtig sein.
- ◊ Tasten mit schwarzer Beschriftung sind zu wählen.
- ◊ Die Verschmutzungsgefahr ist zu beachten." /Kru, S. 25/

2. zur Tastenrückmeldung:
- ◊ "Bewegliche Tasten sollen einen spürbaren Druckpunkt haben.
- ◊ Zusätzliche akustische, in der Lautstärke einstellbare Rückmeldungssignale erleichtern die Arbeit. Tasten müssen einen definierten, konstanten Auslösedruck haben." /Kru, S. 26/

3. zur Tastenanordnung:
- ◊ "Die Beurteilung einer speziellen Tastenanordnung kann nur im Zusammenhang mit der Arbeitsaufgabe erfolgen.
- ◊ Gewohnte Bewegungsmuster sind bei der Wahl neuer Tastenanordnungen zu berücksichtigen.
- ◊ Verschiedene Tastaturen für dieselbe Aufgabe erhöhen die Fehlerrate.
- ◊ Häufig gebrauchte Tasten werden besser in Blöcken als in Zeilen zusammengefasst; denn mehr als 3 x 4 Tasten sind weder mit einem Blick noch mit einer Hand zu erfassen.
- ◊ Für das Programm \`gefährliche´ Tasten sollen außerhalb des zentralen, schnellen Griffbereiches liegen und gegebenenfalls eine Mehrhandbedienung erfordern." /Kru, S. 27/

3.4 Beurteilung der Software, Empfehlungen

Wie schon erwähnt, kann schlecht gestaltete Software zu Stresserscheinungen führen. Schlecht gestaltete Software kann weiterhin Arbeitsvorgänge erschweren und/oder verlangsamen und damit verteuern. Bei der Einführung neuer Software und neuer Softwareversionen darf nicht unterschätzt werden, dass die Anwender einer erhöhten Beanspruchung ausgesetzt sind. Vor allem während der Einführungsphase muss berücksichtigt werden, dass die Mitarbeiter nur bis zu gewissen Grade flexibel sind; beispielsweise sind Rückwirkungen auf die Arbeitsorganisation zu bedenken. Es muss ausreichend Schulungszeit eingeplant sein. Die Ziele `Abbau un-begründeter Ängste´ und `Förderung eines arbeitsbezogenen funktionellen Verständnisses der Software´ müssen wesentliche Punkte der Schulung sein. Untersuchungen und Versuche haben gezeigt, dass schrittweises Lernen mit Übungen gegenüber einem massierten Lernen deutliche Vorteile bietet. Die gerade bei Übungen möglichen Erfolgsrückmeldungen verbessern und beschleunigen das Lernen. /vgl. Kru/
Einheitliche, allgemein anerkannte und objektivierbare Kriterien zur Softwarebeurteilung sind bisher nicht gegeben. Es existieren prinzipielle Vorgaben, deren Interpretation in der Literatur und der Praxis voneinander abweichen. Software sollte folgenden generellen Anforderungen (vgl. DIN 66234 Teil 8) genügen:

⇒*aufgabenangemessen*
Das System (Hardware und Software) sollte an die Anforderungen der Arbeitsumgebung angepasst sein. Eine optimale Arbeitsteilung zwischen Mensch (Anwender) und Maschine (Computer) soll erreicht werden. Das bedeutet zum Beispiel, dass die Software die Arbeit nicht erschweren darf, indem sie zu umständliche Arbeitsschritte vorsieht.
⇒*selbstbeschreibungsfähig*
Die Software muss in der Lage sein anzugeben, was das System unter welchen Bedingungen zu leisten vermag, bzw. gerade durchführt. Im Idealfall sollte das System anwendbar sein, ohne dass vorher eine Beschreibung gelesen werden muss.
⇒*steuerbar*
Dazu gehört die Eigenschaft des Systems, dass beispielsweise je nach Anwenderkenntnissen einzelne Zwischenschritte bei der Menü- oder Dialogführung weggelassen werden können.
⇒*erwartungskonform*
Darunter wird ein konstantes Verhalten und eine fortwährende Zuverlässigkeit des Systems verstanden. Z.B. hat eine bestimmte Eingabe `xyz´ immer die gleiche Reaktion des Programms zur Folge zu haben.

⇒*fehlerrobust*
Ein Computersystem hat nicht bei jeder falschen Handlung des Anwenders abzustürzen, sondern die Software hat diesen Fehler aufzufangen und mittels verständlicher Fehlermeldungen dem Anwender Gelegenheit zu geben, diesen Fehler zu korrigieren.
⇒*einfach*
Darunter fallen: einfache Handhabung, gute Lernhilfen und benutzerangepasste Lernmodi. /vgl. Men/

Dass die oben genannten Anforderungen nicht problemlos zu erfüllen sind - wenn sie überhaupt pauschal erfüllt werden können - liegt schon an der Tatsache, dass verschiedene Benutzergruppen mit einem Programm arbeiten sollen. Das Benutzerprofil (beispielsweise Anfänger, seltener Benutzer, geübter Benutzer, Experte) kann für die Software in der Regel nicht eindeutig festgelegt werden. Software kann unter syntaktischen (Programmaufbau) und unter semantischen (inhaltlichen) Aspekten beurteilt werden. Auf die inhaltlichen Aspekte der hier interessierenden Programme für Arbeitssicherheit kann in gewissen Umfang in den Anforderungen an ein solches Programm eingegangen werden. Hierbei darf jedoch nicht außer acht gelassen werden, dass die inhaltlichen Anforderungen bei solchen Programmen als auch ganz allgemein stark durch die Bedürfnisse des Benutzer geprägt werden. Neben der Zahl prinzipiell möglicher Funktionen ist also die firmenspezifische Funktionalität der Software zu beachten.
Aufgrund der genannten Probleme wird sich im folgenden auf die Möglichkeiten zur Bewertung der Benutzeroberfläche beschränkt. Hierzu existieren einige Erkenntnisse und Regeln (vgl. ISO 9241, Teil 10; DIN 66 234, Teile 3, 5 und 8), die als allgemeine Richtlinien anerkannt sind:

⇒*Informationsanordnung*
“Die auf der Bildschirmoberfläche dargestellte Information soll in wenigen großen Blöcken formal und inhaltlich geordnet sein.
Die Information ist in kleinen Einheiten zu gruppieren, die mit einem Blick erfasst werden können.” /Kru, S. 30/
⇒*Kodierung*
“Mäßiger gezielter Einsatz von Kodierung erleichtert die Arbeit. Wirkungsvolle Kodierungsdimensionen sind Ort, Farbe, Piktogramme.” /Kru, S. 32/ Betrachtet man neuere Software, kann festgehalten werden, dass sich insbesondere die Verwendung von Piktogrammen durchgesetzt hat. Die Regeln für die Verwendung von Farbe, weitere Kodierungsmöglichkeiten und die Vor- und Nachteile der Verwendung von Piktogrammen sind den Bildern 3-9 bis 3-11 angegeben. Bei der Bewertung des Nachteils «zu hoher Platzbedarf» muss

man davon ausgehen, dass 1989 Bildschirme mit 15 Zoll (oder mehr) so gut wie gar nicht benutzt wurden.

Die Kodierung mit Farben
♦ Gut unterscheidbare Farben verwenden. Gesättigte Blautöne vermeiden.
♦ Helligkeitsunterschied größer als 20 cd/m^2 einstellen.
♦ Ausreichenden Leuchtdichtekontrast (1:6, 6:1) wählen.
♦ Große Unterschiede zwischen Farbe und Helligkeit verwenden.
♦ Eine exakte Identifikation ist nur für große Felder möglich (Winkel > 20 min).
♦ Nur auf neutralem Hintergrund tritt keine Farbverfälschung auf.
♦ Gesättigte, helle Farben lassen Objekte größer erscheinen.
♦ Gesättigte, helle Farben großer Wellenlänge vermitteln den Eindruck "Nähe".
♦ Ungesättigte, dunkle Farben kurzer Wellenlänge vermitteln "Ferne".
♦ Nachbarschaft extremer Farben vermeiden (rot/grün, blau/gelb, rot/blau).
♦ Ohne Vergleich können nur 4-6 Farben unterschieden werden.
♦ Mehr als 4-6 Farben erfordern das Angebot einer Vergleichspalette.
♦ Konventionen der Farbkodierung beachten (rot: Gefahr; gelb: Warnung).
♦ Farben können die Aufmerksamkeit erregen, aber auch ablenken.
♦ Farbfehlsichtige können weniger Farben unterscheiden.

Bild 3-10 Regeln, Anmerkungen für die Kodierung mit Farben /Kru/

Kodierungsdimension		Elemente (Beispiele)	(empfehlenswerte) maximale Elementzahl
A	Ziffer	0 1 2 3 4 5 6 7 8 9	10
	Buchstabe	A B C …	Alfabet
B	Kontrast	Leuchtdichtestufe	2
	Helligkeit		2
	Orientierung	Winkel ohne Vergleich	8
	Position	links oben, rechts unten …	9
	Größe	a a a a	3
	Farbe	rot, grün, blau …	6

C	Linien	——— -------	4
	Texturen	Schraffur, Punktierung	3
	abstrakte Formen	Kreis, Rechteck	4
	Piktogramm	Hinweiszeichen	20

Bild 3-11 Die verschiedenen Kodierungsmöglichkeiten /nach Kru/

Vorteile	(mögliche) Probleme
• Anfänger lernen die Grundfunktionen schnell anlässlich einer Demonstration. • Der gelegentliche Benutzer kann leicht operationale Konzepte merken und aktivieren. • Fehlermeldungen werden nur selten benötigt. • Der Benutzer erhält sofort eine Bestätigung über den Erfolg seiner Aktivität. • Der Benutzer hat keine Furcht, weil er das System durchschaut und fehlerhafte Schritte leicht wieder rückgängig gemacht werden können. • Der Benutzer gewinnt schnell Vertrauen und fühlt sich als Herr der Lage. • Die Reaktionen des Systems sind vorhersehbar.	• Graphik benötigt Platz auf dem Bildschirm, der für die eigentlichen Aufgaben fehlt. • Der Vorteil der Anschaulichkeit kann auch durch eine andere Form eines graphischen Modells bei Dialog mit Kommandos erreicht werden. • Der Benutzer muss die Bedeutung der graphischen Komponenten lernen. • Graphiken können doppeldeutig sein und mit bekannten Wissen interferieren. • Der Wechsel der Handposition zwischen Maus und Tastatur behindert den Arbeitsfortgang.

Bild 3-12 Vor- und Nachteile der Piktogramme /Kru/

⇒*Antwortzeiten*

“Je nach Arbeitsaufgabe sollte eine möglichst kurze Antwortzeit bevorzugt werden. Editierbefehle in Textsystemen verlangen kürzeste Antwortzeiten, während für Speicherbefehle längere Zeiten hingenommen werden. Vom Benutzer wird eine kalkulierbare konstante Antwortzeit erwartet, auf die er seinen Arbeitsrhythmus einstellen kann.” Kru, S. 36/

⇒*Fehlermeldung*

Ein wesentlicher Punkt bei der Beurteilung von Software ist die Qualität der Fehlermeldungen. Gute Fehlermeldungen können insbesondere die Einarbeitung in ein Programm deutlich vereinfachen. Gerade wenn Anfänger und gelegentliche Benutzer mit der Software arbeiten müssen, sollte deren Güte im Kriterienkatalog der Beurteilung zur Auswahl der Software mit berücksichtigt werden. D. h. bei der Auswahl der Programme müssen auch die gebotenen Orientierungs- und Korrekturmöglichkeiten berücksichtigt werden. Fehlermeldungen sollten folgende Eigenschaften haben:

- unverschlüsselt,
- fehlerspezifisch und präzise,
- konstruktiv: Antwort auf die Frage, was getan werden muss;
- positive, stimulierende Wortwahl,
- benutzerangepasste Wortwahl,
- gestaffelte Abfolge: Antwort in mehreren Ebenen;
- gleichbleibend in Stil, Terminologie und Abkürzung;
- gleichbleibend bezüglich Format und Position auf dem Bildschirm.

Gleichzeitig sollten sie auch Antworten auf folgende Fragen enthalten:

- Woher bin ich gekommen?
- Wo bin ich?
- Wohin kann ich gelangen?
- Wie korrigiere ich meinen Fehler?

3.5 Beurteilung der Arbeitsumgebung, Empfehlungen

Für die Beurteilung von Büroarbeitsplatz und Arbeitsumgebung existieren eindeutige Vorschriften und Normen. Beispielsweise ist der optimale Bildschirmtisch in der DIN 4543 beschrieben. Der Arbeitsstuhl sollte der DIN 4551 entsprechen. Die Mindestvorschriften zu Tisch und Stuhl sind in der ZH 1/618 zu finden. Diese ZH-Vorschrift beinhaltet auch die Vorgaben zum Vorlagenhalter und empfohlenen Fußstütze. Benutzerflächen und Flächenbedarf der Büroarbeitsplätze sind in DIN 4543 genormt als auch in der ZH 1/535 geregelt. Die Raumbeleuchtung richtet sich nach der Sehaufgabe. Auch hier sollten die Vorschriften ZH 1/535 und ZH 1/618 beachtet werden. In den Prüfungslisten, die sich im Anhang 3-5 finden, werden diese Vorschriften praxisgerecht aufbereitet. Selbstverständlich handelt es sich nur um Vorschläge, wie solche Kontrolllisten aussehen können. Als Mitarbeiter sollte man beachten, dass nach den §§ 16 und 18 des Arbeitsschutzrahmengesetzes die

Mitarbeiter “nach ihren Möglichkeiten sowie gemäß der Unterweisung und der besonderen Weisung des Arbeitgebers für ihre Sicherheit und Gesundheit Sorge zu tragen” haben. Man hat also auch als Mitarbeiter eine gewisse Eigenverantwortung für seine Gesundheit und Sicherheit.

Grundlegende Ratschläge für die Arbeit am Bildschirm

Sie wurden von der Firma Leuwico, die Rechnerarbeitsplätze liefert, direkt übernommen. Im Anhang befinden sich die gesetzlichen Regelungen zu diesem Thema. Weitere Hinweise und Ratschläge ergänzen die grundlegenden Ratschläge.

Eine der wichtigsten Regeln, die man beim Aufstellen eines Bildschirmes beachten muss:

“Bildschirmoberkante nicht über Augenhöhe!



Unnatürliche Augenstellungen und verkrampfte Kopfhaltungen sind wohl die häufigste Ursache von Kopfschmerzen und Verspannungen bei der Bildschirmarbeit. Deshalb ist die Aufstellung der Monitore von ganz entscheidender Bedeutung.

Die Experten sind sich hier einig, ein leicht nach unten geneigter Blick - möglichst auf einen nach hinten geneigten Bildschirm - ist in jedem Fall besser als geradeaus oder nach oben schauen. Stellen Sie den Monitor also besser nicht auf den Rechner, sondern möglichst direkt auf den Tisch.

Die angenehme Blickrichtung ist leicht nach unten, wenn der Bildschirm dabei noch nach hinten geneigt wird, ist der Blickwinkel optimal.

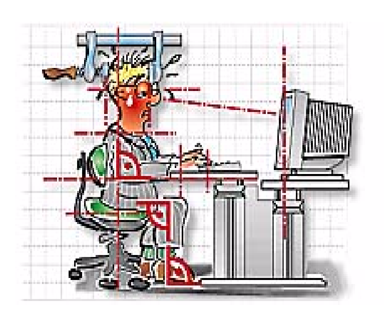


Der Bildschirm sollte so weit vom Auge entfernt sein, wie man es als angenehm empfindet. Bei den meisten Menschen liegt dieser Abstand zwischen 60 und 80 cm. Deshalb ist, insbesondere bei großen Geräten, auf ausreichende Tischtiefe zu achten. Probieren Sie den für Sie angenehmen Abstand aus! Verändern Sie den Abstand, vor allem wenn Sie akute Probleme haben.



Wenn es gar nicht anders geht, muss störender Lichteinfall mit Stellwänden, Lamellenstores, Jalousien o.a. verhindert werden.

Schlechte Lichtverhältnisse werden bei der Bildschirmarbeit schnell zur unerträglichen Belastung. Deshalb gehört es zu den vordringlichsten Aufgaben des Büroplaners, die optimalen Randbedingungen für "gutes" Sehen zu schaffen: Eine angenehme Grundbeleuchtung, ausreichendes Licht auf den unterschiedlichen Arbeitsflächen, die richtige Leuchtdichteverteilung und die Vermeidung von direkter und indirekter Blendung.



Die optimale Arbeitshaltung gibt es nicht. Stunden, ja selbst minutenlang aufrechter Oberkörper, Gliedmaßen im rechten Winkel, Blick geradeaus, ist graue Theorie. Wir brauchen Veränderung, Abwechslung und möglichst oft Bewegung.

Langes Sitzen ist nicht gesund, das hat sich herum gesprochen. Die Bildschirmarbeit birgt also auch für unseren Bewegungsapparat einiges an Gefahren. Lange Sitzphasen und der ständige Blick zum Monitor bringen einseitige statische Beanspruchungen, während auf der anderen Seite hohe mentale Anforderungen gestellt sind. Wir sollten also darauf achten uns regelmäßig zu bewegen, auch bei langen Rechnersitzungen. Ein guter Stuhl, der dynamisches Sitzen fördert ist hier sicher hilfreich.



Mal eben kurz aufstehen, das tut allen Muskeln gut. Der spontane Wechsel der Körperhaltung zwischen Sitzen und Stehen sollte zum Büroalltag gehören.

Noch effektiver sind Bildschirmarbeitstische die wechselnde Arbeitshaltung bis hin zum Stehen möglich machen. In jedem Fall gilt unser Tipp: Jede Bewegungsmöglichkeit, die sich bietet, nutzen - so ist die Chance groß, dass Sie den Arbeitsplatz fit und zufrieden und nicht abgespannt verlassen.



So sieht entspanntes Arbeiten am Bildschirm nicht aus.

Die zur Verfügung stehenden Arbeits- und Bewegungsflächen müssen den menschlichen Körpermaßen angepasst sein. Auf der einen Seite sollte man sich frei bewegen können auf der anderen sollten die wichtigen Arbeitsmittel bequem greifbar sein. Versuchen Sie die Anordnung von Bildschirm, Tastatur, Vorlagen und anderen Arbeitsmitteln Ihrem Arbeitsablauf anzupassen. Vermeiden Sie es insbesondere, ständig zur Seite auf den Monitor zu schauen.

Genauso wichtig wie genügend Arbeitsfläche ist Bewegungsfreiheit. Wer sich beengt fühlt, fühlt sich meist auch unwohl.

Deshalb sollten die einschlägigen Vorschriften zum Flächenbedarf am und um den Arbeitsplatz unbedingt beachtet werden.
Darüber hinaus muss gutes Bürolayout eine ganze Reihe weiterer Aspekte berücksichtigen. Von der Organisations- und Kommunikationsstruktur über das Tätigkeitsprofil bis hin zu den individuellen Bedürfnissen der Anwender." /Leu, S. 1-3/

Ein Mensch aus einem Labor rief bei uns an, und schilderte uns ein äußerst merkwürdiges Problem. Morgens würde der Monitor einwandfrei funktionieren, mittags auch noch, aber jeden Nachmittag würde er ausfallen. Möglicherweise ein Wärmefehler?
Also dort ins Labor gefahren, Ersatzmonitor mit dabei. Will die Geräte gerade austauschen... Da! Was ist das?! Der Monitor hing an ein einer Steckdose, in welcher eine Zeitschaltuhr steckte, eingestellt auf 16:00 Uhr ausschalten.
From: Maja Hulicka, maja.hulicka@zx.x400.basf-ag.de

4 Datenschutz und Datensicherheit

Das Aufgabengebiet `Datenschutz´ wird gerade in kleinen und mittleren Betrieben gern dem Aufgabenfeld einer Fachkraft für Arbeitssicherheit zugeschlagen. /Sche1/ Selbst wenn dies nicht der Fall sein sollte, ist dieses Thema für die Fachkraft für Arbeitssicherheit interessant. Denn in einer Untersuchung wurde ermittelt, dass fast 90 % der Fachkräfte für Arbeitssicherheit mit EDV arbeiten. Und in der Regel werden von ihnen personenbezogene Daten oder/und andere vertrauliche betriebsinterne Daten per EDV gespeichert und verarbeitet./Sche1/ Daher sollte eine Fachkraft für Arbeitssicherheit aus eigenem Interesse im Bereich Datenschutz die wichtigsten Begriffe beherrschen und die wesentlichen gesetzlichen Grundlagen kennen.
Aus fast den gleichen Gründen ist es notwendig, als Fachkraft für Arbeitssicherheit sich auch bei der Datensicherheit auszukennen. Dazu kommen Ereignisse (vgl. hierzu Kapitel 4.2), die zum Teil schon recht häufig aufgetreten sind und wie man aus eigener Erfahrung weiß und/oder eigener Überlegung abschätzen kann, aus Gedankenlosigkeit, Bequemlichkeit, Leichtsinn oder Unwissenheit sowie aus Verschleißgründen und Fertigungsproblemen immer wieder geschehen.
Worin liegt nun jedoch der Unterschied zwischen Datensicherheit und Datenschutz? Antwort geben in Kapitel 4.1 das DIN und eine Erläuterung von Hans Wohlgemut.

4.1 Definition von Datensicherheit, -sicherung und -schutz

In der DIN 44300 werden die Termini Datensicherheit und Datensicherung wie folgt definiert:

⇒ Datensicherheit ist der Schutz der Daten vor z.B. Verlust, Missbrauch oder ähnlichem.

Bei der Datensicherung geht es nicht nur um personenbezogene Daten, sondern um Daten jeglichen Inhalts; dies können z.B. im kaufmännischen Bereich Einkaufspreise, Kalkulationen etc. sein oder im sicherheits-technischen Umfeld können dies auch Stoffwerte, Berechnungen und/oder Risikoanalysen sein. /vgl. Woh und Gro/

⇒ Datensicherung sind die hierfür notwendigen Maßnahmen.

Bei der Datensicherung geht es um die Realisierung der Datensicherheit, aber auch der Datenschutz soll als Ziel erreicht werden. Für zwei unterschiedliche Ziele werden also die gleichen Maßnahmen ergriffen. Dies ist auch der Grund, warum Datensicherheit und Datenschutz im gleichen Kapitel behandelt werden.
Es sollen also Verfügbarkeit, Vertraulichkeit und Integrität der Daten gewährleistet werden; in anderen Worten, es geht um die physische

Aufrechterhaltung des DV-Betriebes und der Abwehr von Datenmissbrauch und Datenverfälschung. /vgl. Woh und Gro/

⇒ Datenschutz ist der Schutz der Persönlichkeit vor dem Missbrauch seiner persönlichen Daten.

Unter Datenschutz versteht man nicht den Schutz der Daten an sich, sondern vielmehr den des Betroffenen vor einem bestimmten Umgang mit den Daten, die sich auf seine Person beziehen. Es geht um den Schutz des Persönlichkeitsrechts. Betroffen ist derjenige, auf den sich die ent-sprechenden Daten beziehen. Im Rahmen des Datenschutzes wird jeder Umgang mit diesen Daten betrachtet. Es interessieren die einzelnen Verarbeitungsphasen `Aufnahme, Speicherung, Veränderung, Übermittlung, Sperrung und Löschung aber auch der Vorgang der Datenerhebung und die nicht rechnergestützte Übermittlung sowie die Verwendung beziehungsweise Nutzung der ermittelten Daten. /vgl. Woh/

4.2 Mögliche Gefahren bei der Datenverarbeitung

G. Aleanakian und W. Kühnau haben /Ale/ in einer anschaulichen Beispielsammlung verschiedene Möglichkeiten zusammengestellt, die bei der Datenverarbeitung zu Schäden führen können und auch schon führten. Diese Beispiele reichen von ungewollten Benutzerfehlern, ungeschickter Aufstellung des Rechners über Software- und Hardwarefehler und dem bewussten Missbrauch bis hin zu Schäden durch Höhere Gewalt. In den Bildern 4-1 bis 4-4 werden die Beispiele nach der Gefährdungskette aufgeschlüsselt. Im Einzelnen können dies sein:

- ungewollte Benutzerfehler:	-- Tippfehler -- ungewolltes Datenlöschen -- Getränkverschütten auf der Tastatur
- schlechte Aufstellung:	-- PC hat direkte Sonnenbestrahlung
- Softwarefehler:	-- Unvorhersehbare Systemabstürze
- Hardwarefehler:	-- Diskettenlaufwerk liest nicht -- Inkompatibilität diverser Komponenten
- bewusster Missbrauch:	-- Datendiebstahl -- gewolltes Löschen wichtiger Daten
- Höhere Gewalt:	-- Krankheit, Ausfall eines Mitarbeiters -- Wetterschäden -- Stromausfall

Gefahr/ Gefährdung	Auslösung	Schädigung	Schaden	Folgeschaden
Benutzer	unbewusst, durch Eingabefehler	z.B. Löschung der Texte	Verlust von möglicherweise wichtigen Texten	Aufwand für die Neuerstellung der Texte, Schaden durch Fehlen der Texte
Benutzer	zufällig, aus Versehen	Zerstörung der Tastatur	Ausfall des PC	Kosten für die Tastatur und die Ausfalldauer
Betreiber	unabsichtlich, wegen falscher Aufstellung	Abbruch der Verarbeitung	Ausfall des PC	Kosten für die Ausfalldauer, eventuell Reparatur

Bild 4-1 Anwenderfehler /nach Ale/

Gefahr/ Gefährdung	Auslösung	Schädigung	Schaden	Folgeschaden
Software	zufällig, durch Programmfehler	Abbruch der Verarbeitung (in bestimmten Situationen)	Minderung der Funktionsfähigkeit	Beseitigung des Fehlers, Ärger, Zeitaufwand bis zur Beseitigung
Hardware	zufällige Fehlfunktion	Verfälschung der Hardwarefunktionen	Disketten sind nicht lesbar	fehlende Daten, Neujustierung
technisches System	zufällig, durch Inkompatibilität	Verfälschung der Funktion des Textsystems	Texte können nicht gedruckt werden	Fehlerbeseitigung, Zeitaufwand

Bild 4-2 Fehlfunktionen /nach Ale/

Eine Sekretärin hat mal angerufen, weil der Rechner nicht mehr gebootet hat und nur wilde Zeichen zu sehen wären. Auf die Frage, was denn auf dem Monitor steht, kam prompt die Antwort: "Ne Tasse Kaffee."
From: "frerk@informatik.uni-kl.de"

Gefahr/ Gefährdung	Auslösung	Schädigung	Schaden	Folgeschaden
Mensch	bewusst, durch Diebstahl	Einsicht-nahme in vertrauliche Daten	Daten werden entgegen den Wünschen des Betriebes verwendet	Schwächung der Konkurrenz-fähigkeit
Mitarbeiter	bewusst, durch Sabotage	Löschung von Daten	Verlust von wichtigen Daten	Zeitaufwand (Behinderung bei der Arbeit), Aufwand für Aufklärung und Wiederher-stellung

Bild 4-3 Missbrauch /nach Ale/

Gefahr/ Gefährdung	Auslösung	Schädigung	Schaden	Folgeschaden
Umwelt	zufällig, wegen Krankheit eines Mitarbeiters	Fehlen der Mitarbeiter mit PC-Kenntnissen	Ausfall des Systems	Überstunden, geringere Qualität, Verspätungen
Umwelt	zufällig, Sturm	Zerstörung der Hardware	Ausfall des Systems	Kosten für Reparatur, neue Geräte, Ausfalldauer
technische Umwelt	zufälliger Stromausfall	Abbruch der Verarbeitung, Löschen der Daten im Haupt-speicher	Verlust des gerade eingegebenen Textes	Wiederholung der Arbeit

Bild 4-4 Höhere Gewalt /nach Ale/

Wie die Beispiele zeigen kann man nach äußeren und inneren Gefahren unterscheiden. Hauptgefahrenquelle ist wohl der Mensch an sich selbst (bewusst oder unbewusst), dazu kommen die Unwägbarkeiten der Natur/Umwelt und

des technischen Systems. Auslöser sind oft Anwendungsfehler, auch Fehlfunktionen, Missbrauch und höhere Gewalt spielen eine wichtige Rolle. Ähnliche Gefahrenquellen, aber auch andere Risken zeigt M. Lackmann /Lac/ in seinem Bericht über durchgeführte Computerrevisionen. Hier sollen nur Stichworte die wichtigsten Ergebnisse der Revisionen beschreiben, die sich in Form von Sicherheitsrisiken und -defizite auswirken:

- Abweichung der Hardware vom Sollzustand
- Abweichung der Software vom Sollzustand
- Fehlerhafte Verzeichnisstruktur
- Häufig Abweichungen von den Konfigurationsdateien (Config.sys; Autoexec.bat und Net.cfg in der DOS-Welt)
- Fehlende organisatorische Regeln und Vorschriften
- Gebrauch von unlizenzierten Kopien
- Gebrauch von (nicht genehmigten) Spielprogrammen
- Software vorhanden, die so gut wie nie benutzt wird
- Zugriffschutzsysteme nicht genutzt
- Zu großzügige Rechtevergabe im LAN
- Terminals (und PCs) häufig unbeaufsichtigt gelassen
- Datenbanken angelegt ohne Sicherungskopien
- Keine regelmäßigen Datensicherungen
- Sicherungskopien nicht sorgfältig aufbewahrt
- Einsicht in Daten möglich, die verschlüsselt sein müssten
- Ungenügende (physikalische) Löschung von Daten
- Virenbefall auf PCs sowie in Netzwerken /vgl. Lac, S. 5 ff./

Die hier erwähnten Mängel sind zum Teil organisatorische Fehler, zum Teil liegen sie an der mangelnden Schulung und Information der Mitarbeiter und einige Mängel sind den einzelnen Mitarbeitern anzulasten. Der \`Fehler´ ungenügende physikalische Löschung von Daten kann sogar als \`Vorteil´ erwünscht sein, denn oft werden Daten ohne Absicht gelöscht oder das Löschen wird als Fehler erkannt. In vielen Fällen können Daten so gerettet

> Ein Benutzer kommt in die Beratung.
> Benutzer: "Nebenan im PC-Pool ist alles voll, und der einzige Rechner der noch frei ist geht nicht."
> Berater: "??? Ich schau mir das mal an."
> Berater untersucht den PC. Keine Tastatur-Eingabe erscheint auf dem Bildschirm. Alle Kabel sitzen bombenfest. Ein Reset hilft auch nicht weiter. Der Berater dreht die Tastatur um, um zu gucken ob die vielleicht versehentlich auf XT statt AT gestellt ist. Als er sie wieder hinlegen will, sieht er den aus der Tastatur herausgeflossenen kalten Kaffee. ...
> Und er trug die Tastatur in die Hardware-Abteilung mit den Worten: "Könnt Ihr die grad mal trocken föhnen??"
> From: "IWS88116@ibm.rz.uni-passau.de"

werden. (Wären Sicherungskopien gemacht, wären die hierfür notwendigen Aufwendungen zur Rettung von Daten nicht notwendig)
Viren können durch verseuchte Software, aber auch über das Netz eingeschleust werden. Auf das Thema `Viren´ wird in Kapitel 5 ausführlicher eingegangen. Andere Gefahren der Netzwerkbenutzung und der Datenübertragung per Netz werden von W. J. Jaburek /Jab/ in seiner Dissertation `Risiken elektronischer Datenübermittlung ... ´ dargestellt. Auch hier werden in einigen Stichworten die wesentlichen Gefahren aufgezählt:

- Mitarbeiter
  -- Fehlbedienung
  -- Kennwortverrat
- Geräte/Programme
  -- Ausfall
  -- Speicherung der Daten im Klartext
  -- Abstrahlung des Bildschirm; Angezeigte Daten können mit speziellen Geräten bis zu einem Kilometer entziffert werden; bei geheimen Daten von Interesse (z.B. Bankdaten)
- Das Netz selbst
  -- Ausfall eines Übertragungselementes
  -- Stromschwankungen
  -- Verschiedene Abhörmöglichkeiten

W. J. Jaburek hat die Fälle ausführlich geschildert und auch Lösungsvorschläge angegeben, wie solche Fälle vermieden werden können. Wie Aleanakian/ Kühnau macht er Vorschläge für Prüflisten und Fragekataloge, die helfen sollen, die Datenorganisation übersichtlicher zu machen.
Soweit zu den Gefahren, die bei der Datenverarbeitung auftreten können und auch immer noch andauernd zu Problemen, Verzögerungen und Pannen führen.
Ausschlaggebend für eine gesetzliche Regelung der Datensicherheit und des Datenschutzes waren jedoch politisch geprägte Überlegungen, die unter anderem von Hans Wohlgemut und Michael Kloepfer /Kloe/ beschrieben und erläutert werden und hier erwähnt werden, ohne sie zu diskutieren:
“Die Entwicklung der modernen, insbesondere computergestützten Informationstechnik bringt bestimmte Gefahren mit sich, die zu beseitigen oder doch zumindest einzudämmen u.a. Aufgabe des Datenschutzes ist. Dabei hält die Geschwindigkeit der informationstechnischen Entwicklung unvermindert an, sie wird zudem massiv durch finanzielle Mittel der öffentlichen Hand gefördert. Dies hat zur Folge, dass die Computertechnik in immer stärkerem Umfang Einzug in die Betriebe und Verwaltungen hält und damit zur Erfüllung von immer mehr Aufgaben eingesetzt wird.

Was die mit dem Einsatz der Informationstechnik verbundenen Gefahren anbelangt, so sind folgende hervorzuheben:

⇒ Der Einsatz informationstechnischer Systeme führt zu einer Verschiebung im gesellschaftlichen Machtsystem und gibt beispielsweise der Ministerialbürokratie einen Vorsprung dem Parlament gegenüber. Allgemein bewirkt er eine Verstärkung der Planungs-, Regulierungs- und Kontrollmacht des \`Systemherrn´. Informationssysteme wirken als Machtverstärker, indem sie die von der Datenverarbeitung Betroffenen als \`Datenobjekte´ in höherem Maße als zuvor zugunsten des Systemherrn verfügbar, ja manipulierbar machen.

⇒ Im Bereich des Arbeitslebens ermöglicht der Einsatz der Informationstechnik eine Systematisierung und Effektivisierung der Personalplanung und Personalverwaltung entsprechend den vom Arbeitgeber verfolgten Zielen. Der Einsatz der betrieblichen Datenerfassung und -verarbeitung steigert so die Abhängigkeit des Arbeitnehmers vom Arbeitgeber. Die systematische Langzeitüberwachung durch ständiges Messen und Vergleichen der Leistung Einzelner bzw. von Gruppen und die kontinuierliche Beobachtung und Aufzeichnung ihres Verhaltens geben dem Arbeitgeber einen umfassenden Überblick und letztlich eine breite Palette von Handlungs- und Bewertungsmöglichkeiten für bestimmte Maßnahmen an die Hand.

⇒ Wie das Bundesverfassungsgericht hervorgehoben hat, erzeugt der Einsatz der Datenverarbeitung einen Konformitätsdruck zu Lasten der Betroffenen, welcher grundgesetzbeeinträchtigend wirkt. Dies hat das Gericht eindringlich mit folgenden Worten beschrieben: \`Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden."

/Woh, Kloe, vgl. Woh, S.2 ff. und Kloe, S. 37 ff./

4.3 Das Bundesdatenschutzgesetz

Ausführlich wird das Bundesdatenschutzgesetz in einer Schrift der Gesellschaft für Datenschutz und Datensicherung (GDD) /GDD/ abgehandelt, die auch als Quelle diente. In diesem Buch wird sich auf die Paragraphen des Gesetzes beschränkt, die für die Arbeit einer Fachkraft für Arbeitsicherheit von direktem Interesse sind. (die Paragrafen des Gesetzes, die für eine FaSi wichtig sind, sind im Anhang zu finden, dort findet sich auch eine Internettadresse, wo man das Gesetz einsehen kann)

Das Bundesdatenschutzgesetz ist als Auffanggesetz konzipiert. Das heißt, dass die Vorschriften des Bundes, die Verbote und Gebote über die Erhebung, Verarbeitung, Nutzung sowie den Schutz personenbezogener Daten enthalten, vor dem Bundesdatenschutzgesetz Vorrang genießen. Beispiele für vorrangige Rechtsvorschriften sind:
- Bestimmungen über die ärztliche Schweigepflicht
- Betriebsverfassungsgesetz
- Lohnsteuervorschriften, - Statistikgesetze
- Sozialgesetzbücher
- Zivilprozessordnung /vgl. hierzu GDD, S. 12 und 13/

Das Gesetz ist in sechs Abschnitte gegliedert:
1. Allgemeine Vorschriften (Aufgabenbereich, Definitionen, Rechte der von der Datenverarbeitung Betroffenen)
2. Vorschriften für die Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen
3. Vorschriften für die Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen für eigene Zwecke und die geschäftsmäßige Datenverarbeitung
4. Sondervorschriften (Wissenschaft, Mediennutzung, Geheimnisschutz)
5. Straf- und Bußgeldvorschriften
6. Übergangs- und Schlussvorschriften

4.3.1 Zweck und Anwendungsbereich des Gesetzes (§ 1 BDSG)

Aufgabe und Gegenstand des Gesetzes ist der Datenschutz; das Ziel ist nicht der Schutz der Daten als Selbstzweck, sondern der Schutz der Persönlichkeitsrechte des Einzelnen vor dem Missbrauch seiner persönlichen Daten. Geregelt werden Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Unter personenbezogenen Daten versteht man z.B. Einzelangaben (also in der Regel keine Summendaten) über

- persönliche Verhältnisse, z.B. Familienstand, Geburtsdatum
- sachliche Verhältnisse, z.B. Besitz, Verträge
-- einer bestimmten, z.B. namentlich benannten
-- einer bestimmbaren, z.B. über Personalnummer erkennbaren
- natürlichen Person, z.B. Arbeitnehmer, Einzelkaufmann etc.

nicht aber GmbH, AG, OHG, KG, politische Parteien, Gewerkschaften etc.

Dabei gliedert sich die Verarbeitung in fünf sogenannte `Phasen´, nämlich das Speichern, das Verändern, das Übermitteln, das Sperren und das Löschen. Zu beachten ist hierbei, dass nicht die technische Deutung dieser Worte ausschlaggebend ist, sondern deren juristische Interpretation. Sie werden als

Beschreibung für Vorgänge verwendet, "die der Gesetzgeber besonderen Zuverlässigkeitsvoraussetzungen unterworfen hat."/GDD, S. 12/
Nicht-personenbezogene Daten wie z.B. Materialdaten, Lagerbestandsdaten, Sortimentsdaten, Stücklistendaten, produktbezogene Produktionsdaten, Planungsdaten, die sich nicht auf den einzelnen Mitarbeiter beziehen, wie Finanzplanung und Umsatzplanung sowie statistische Daten fallen nicht unter das Bundesdatenschutzgesetz.
Daten in Akten, Aktensammlungen und in Registraturen fallen nur dann in den Geltungsbereich des Bundesdatenschutzgesetzes, wenn sie durch automatische Verfahren umgeordnet und ausgewertet werden können. (z.B. automatischer Index)
Daten über juristische Personen (z.B. über Aktiengesellschaften [AG], Gesellschaften mit beschränkter Haftung [GmbH]) und Daten, die nicht in einer Datei im Sinne des Bundesdatenschutzgesetzes (§3 Abschnitt 2) gespeichert werden, fallen ebenfalls nicht unter das Bundesdatenschutzgesetz.

4.3.2 Weitere Begriffsbestimmungen (§ 3 BDSG)

Das Bundesdatenschutzgesetz regelt eine Materie, die bisher technisch beschrieben war. Um nun einen gemeinsamen Sprachgebrauch von Technikern, Juristen und Anwendern zu ermöglichen, werden im dritten Paragraphen des Gesetzes wichtige Termini bestimmt. Einige der Definitionen zur Datenverarbeitung und deren einzelnen Phasen `Speichern, Verändern, Übermitteln, Sperren und Löschen´ und zur Datennutzung werden exemplarisch besprochen:
" 1. Speichern
Erfassen, Speichern (Anm.: im technischen Sinne), Aufnehmen oder Aufbewahren von personenbezogenen Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung.
Wichtig: Ziel der Speicherung auf Karteikarten, Lochkarten, Eingabe in den Computer ist die Verarbeitung oder Nutzung in der Datei.
2. Verändern
Inhaltliches Umgestalten gespeicherter Daten, z.B. des Fortschreiben der Jahressummen oder der Lohngruppe, Namensänderungen oder Wohnortwechsel; ggf. auch das Hineinstellen in einen neuen Kontext.
3. Übermitteln
Vorgang der Bekanntgabe von personenbezogenen Daten aus einer Datei an Dritte durch aktive Weitergabe. Unerheblich ist die Form der Übermittlung: mündlich, schriftlich, Datenträgerversand, Überleitungen etc.
Eine Übermittlung liegt bei Daten, die zur Einsicht oder zum Abruf bereitgehalten werden (Online-Verfahren) erst dann vor, wenn der Empfänger diese auch tatsächlich einsieht oder abruft.

4. Sperren
Kennzeichnen gespeicherter Daten, um die weitere Verarbeitung und Nutzung einzuschränken. Der entsprechende Vermerk kann in einem Hinweis in bestimmten Datenbeständen oder auf einem Datenträger bestehen. Die Verarbeitung oder Nutzung gesperrter Daten ist bis zu ihrer Entsperrung oder endgültigen Löschung nur unter sehr engen Voraussetzungen möglich.
5. Löschen
Unkenntlichmachen gespeicherter Daten. Das Löschen erfolgt durch physikalisches Vernichten von Datenträgern (z.B. Karteikarten) oder durch das `Entfernen der Daten´ vom Datenträger (z.B. Überschreiben von Magnetbändern). Einzeldaten von Karteikarten können gesperrt werden. Bei magnetischen Datenträgern (Disketten, Festplatten, Magnetbändern, Bandkassetten, Platteneinheiten) ist zu beachten, dass zwischen logischem und physischen Löschen ein wichtiger Unterschied besteht. Nur das physische Löschen versteht das BDSG unter `Löschen´. Wer aber beispielsweise auf einem PC mit dem ERASE- oder DEL-Befehl arbeitet, der löscht nur den Eintrag im Inhaltsverzeichnis. Die Datei bleibt solange gespeichert, bis das Betriebssystem den freigewordenen Speicherplatz neu belegt und dabei überschreibt.
Auch der FORMAT-Befehl, der unter dem Betriebssystem MS-DOS einen ganzen Massenspeicher löscht (Anm.: im technischen Sinne), wirkt höchst unterschiedlich: Eine damit behandelte Diskette wird überschrieben (bis MS-DOS 4.01; ab Version 5.0 ist auch dies nicht gewährleistet), während bei der Festplatte nur das Inhaltsverzeichnis gelöscht wird. Da es Software gibt (Norton Utilities, PC-Tools), die derart `gelöschte´ Dateien reaktivieren können, sind dem Benutzer klare Anweisungen (je nach benutztem System) zu geben, wie er wirkungsvoll Daten zu löschen hat.
Nur diese Phasen sind Datenverarbeitung im Sinne des BDSG! Unerheblich ist, ob die Daten in herkömmlichen Karteien oder automatisiert verarbeitet werden.
Nutzung (Abs. 6)
Unter Nutzen versteht das BDSG jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt. Dadurch soll der gesetzliche Schutzzweck über die Phasen der Datenverarbeitung hinaus auf den Gebrauch von Daten unmittelbar aus einer Datei ausgedehnt werden. Die Nutzung steht gleichrangig neben der Erhebung und Verarbeitung."
/GDD, S. 14 und15/

4.3.3 Zulässigkeit der Datenverarbeitung und -nutzung (§ 4)

"§ 4 enthält ein sogenanntes `Verbot mit Erlaubnisvorbehalt´." /GDD, S.16/
Das heißt die Verarbeitung personenbezogener Daten ist verboten, außer sie wird ausdrücklich erlaubt. Die Verarbeitung und Nutzung personenbezogener

Daten ist also nur bei Vorliegen bestimmter Erlaubnistatbestände zulässig; vgl. hierzu auch § 14 Bundesdatenschutzgesetz; z.B. wenn andere Rechtsvorschriften gelten (HGB, ZPO etc.) und/oder eine schriftliche Einwilligung des Betroffenen vorliegt. /vgl. GDD S. 16 u. 17/

4.3.4 Datengeheimnis (§ 5)

Alle Mitarbeiter, die personenbezogene Daten - auch nur als Teil ihrer Arbeit - in oder aus Dateien im Sinne des Gesetzes verarbeiten und/oder nutzen, sind auf das Datengeheimnis zu verpflichten. Sie haben also über die personenbezogenen Daten, die ihnen aufgrund ihrer Tätigkeit bekannt wurden, Stillschweigen zu bewahren. Dies sind insbesondere:
"- Mitarbeiter in allen Bereichen, in denen PCs im Einsatz sind
- Mitarbeiter der Rechenzentren
- Mitarbeiter in Fachabteilungen mit personenbezogenen Daten wie z.B.:
  - Personalleitung, Lohn- und Gehaltsabrechnung, Zeitwirtschaft
  - Verkauf, Marketing, Werbung
  - Einkauf
  - Controlling" /GDD, S. 17/

4.3.5 Unabdingbare Rechte des Betroffenen (§ 6)

§ 6 Bundesdatenschutzgesetz ist im Zusammenhang mit den §§ 19, 20, 34 und 35 zu sehen. Die in diesen §§ beschriebenen Rechte können nicht durch Rechtsgeschäfte aufgehoben oder beschränkt werden.
Nach diesen §§ hat jeder das Recht auf Auskunft über
- die Daten, die zu seiner Person gespeichert sind und über
- die regelmäßigen Empfänger dieser Daten im Falle automatischer Datenverarbeitung.

Jeder Betroffene hat außerdem das Recht auf Korrektor der Daten, wenn
- sie unrichtig sind; das heißt sowohl der Betroffene als auch die speichernde Stelle haben die gespeicherten Daten als falsch erkannt.

Der Betroffene kann eine Sperrung der Daten verlangen, wenn
- sich weder Richtigkeit noch Unrichtigkeit der Daten feststellen lassen und/oder
- die ursprünglich erfüllten Voraussetzungen für die Speicherung weggefallen sind.

Er kann eine Löschung der Daten verlangen, wenn
- Die Speicherung unzulässig war und/oder
- die ursprünglich erfüllten Voraussetzungen für die Speicherung weggefallen sind.

Die Löschung der Daten ist hier die Alternative zum Recht auf Sperrung.

4.3.6 Technische und organisatorische Maßnahmen (§ 9)

In diesem Paragraph und der damit verbundenen Anlage werden konkrete Maßnahmen zur Datensicherung vorgegeben, die den Schutz der Daten vor unbefugtem Zugriff oder ungewollten Verlust bezwecken. In Kapitel 4.4 wird hierauf genauer eingegangen.

4.3.7 Datenspeicherung, -übermittlung und Datennutzung für eigene Zwecke (§ 28)

Personenbezogene Daten (aus Dateien) dürfen übermittelt werden im Rahmen der Zweckbestimmung eines Vertragsverhältnisses (mit den Betroffenen) und im Rahmen der Zweckbestimmung eines vertragsähnlichen Vertrauensverhältnisses (mit den Betroffenen).
Wenn es zur Wahrung berechtigter Interessen der übermittelnden Stelle oder eines Dritten oder der Allgemeinheit notwendig sein sollte, ist die Speicherung und Übermittlung von Daten ebenfalls zulässig, soweit nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.
Die Weitergabe und Nutzung von Daten über Angehörige einer Personengruppe, die listenmässig zusammengefasst sind, ist erlaubt. Die Daten haben sich auf Name, Titel, akademische Grade, Geburtsdatum, Berufs-, Branchen- oder Geschäftsbezeichnung, Anschrift und Rufnummer zu beschränken und es muss davon ausgegangen werden können, dass schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. /vgl. GDD, S. 23 ff./

4.3.8 Bestellung eines Beauftragten für den Datenschutz (§ 36)

“Jedes Unternehmen, das personenbezogene Daten verarbeitet, hat von einer bestimmten Größenordnung an einen `Beauftragten für den Datenschutz´ (DSB) zu bestellen und zwar dann, wenn es

- personenbezogene Daten verarbeitet und
- hiermit im automatisierten Verfahren mindestens fünf oder
- im nicht-automatisierten Verfahren mindestens zwanzig
  Mitarbeiter ständig beschäftigt. ...

Dem Datenschutzbeauftragten (DSB) ist durch das Gesetz eine herausgehobene Position im Unternehmen eingeräumt worden:

- unmittelbare Anbindung an die Geschäftsleitung
- Verpflichtung der Geschäftsleitung, ihn zu unterstützen
- Weisungsfreiheit bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes
- Benachteiligungsverbot bezüglich der Erfüllung seiner Aufgaben
- besonderen Abberufungsschutz
- besondere Verschwiegenheitsverpflichtung.” /GDD, S. 36, 37/

Die Funktion des Datenschutzbeauftragten kann u.a. in Abhängigkeit von der Betriebsgröße verschieden ausgefüllt werden. In Großunternehmen wird in der Regel ein Datenschutzbeauftragter bestellt, der ausschließlich Datenschutzaufgaben wahrnimmt. Häufiger wird der Datenschutzbeauftragte noch andere betriebliche Aufgaben wahrnehmen. Eine Möglichkeit ist auch die Bestellung eines externen Datenschutzbeauftragten. Personen mit Leitungsfunktion oder Personen, die bei dieser Tätigkeit Interessenskonflikten ausgesetzt wären, sollten nicht zum Datenschutzbeauftragten berufen werden. Der Datenschutzbeauftragte kann nur aufgrund einer Aufforderung der Aufsichtsbehörde oder durch die Anwendung des Paragraphen 626 BGB (`fristlose Kündigung aus wichtigem Grund´) abberufen werden.
Um als Datenschutzbeauftragter berufen zu werden, sollte die entsprechende Person folgende Fähigkeiten besitzen:

- die Datenschutzproblematik verstehen,
- die Geschäftszwecke und Ziele des Unternehmens kennen und verstehen, dessen Interessen er auch als Datenschutzbeauftragter zu vertreten hat,
- fähig sein, Fragen der Organisation, der Revision, der Datenverarbeitung und der Fachabteilungen zu beurteilen,
- wissen, wann das eigene Wissen zur Klärung anstehender Fragen nicht mehr ausreicht und er sich deshalb des Rates von Fachleuten bedienen muss,
- fähig sein, eine Güterabwägung durchzuführen zwischen den schutzwürdigen Belangen des Betroffenen und den berechtigten Interessen
  - des Unternehmens
  - eines Dritten (z.B. einer Zulieferfirma)
  - der Allgemeinheit (z.B. an einem reibungslos laufenden Wirtschaftsgeschehen).

Er muss also vor allem Managereigenschaften haben; er braucht kein Spezialist der EDV oder anderer Fachgebiete zu sein. Steht bei einer überraschenden Neubestellung eines Datenschutzbeauftragten kein Kandidat zur Verfügung, der von Anfang an alle oben erwähnten Voraussetzungen erfüllt, reicht es aus, wenn er die Fähigkeit besitzt, sich in andere Gebiete einzuarbeiten. /vgl. GDD, S. 39 ff. und Lin/

4.3.9 Aufgaben des Beauftragten für den Datenschutz (§ 37)

Der Datenschutzbeauftragte hat eine zentrale Rolle bei der Durchsetzung und Kontrolle des Datenschutzes im Unternehmen. Er hat die Umsetzung der Vorschriften des Bundesdatenschutzgesetzes sicherzustellen, wenngleich die letztendliche Verantwortung bei der Geschäftsleitung liegt.

Im einzelnen gehört (in geraffter Form dargestellt) zu seinen Aufgaben (vgl. GDD, S 38 ff, und Lin):

⇒Die Überwachung der Datenverarbeitungsprogramme. Dies kann durch Testläufe, Systemchecks und Stichprobenkontrollen erfolgen. Werden aus anderen Gründen (Revision, Wirtschaftlichkeitsprüfung etc.) ohnehin EDV-Kontrollen durchgeführt, kann der Datenschutzbeauftragte den Prüfer bitten, Datenschutzaspekte zu berücksichtigen und ihm die Ergebnisse mitzuteilen.

⇒In Planung befindliche DV-Vorhaben, die der Verarbeitung personenbezogener Daten dienen, sind im Vorfeld daraufhin zu prüfen, ob datenschutzrelevante rechtliche Aspekte berührt und daher auf die Planung Einfluss genommen werden muss.

⇒Schulung der Mitarbeiter oder die Erstellung der Vorgaben der Schulung der Mitarbeiter zum Thema Datenschutz. Dazu gehören auch Unterweisungen am Arbeitsplatz sowie Einzel- und Gruppengespräche, die Verständnis für die Belange des Datenschutzes wecken sollen.

⇒Die Beratung z.B. der Personalabteilung bei der Einstellung von Personen, die in der Datenverarbeitung tätig sein sollen.

⇒Verschaffen eines Überblicks, wo im Unternehmen welche Daten verarbeitet werden.

⇒Verschaffen eines Überblicks über die für das Unternehmen in Betracht kommenden Datenschutzvorschriften.

Ausführliche Informationen zu den Aufgaben eines Datenschutzbeauftragten enthält das Handbuch von Koch "Der betriebliche Datenschutzbeauftragte". Dieses Buch wird von der GDD empfohlen und enthält weitere wertvolle Hinweise zu den Aufgaben, aber auch zu den Anforderungen an und Voraussetzungen der betrieblichen Datenschutzbeauftragten.

4.4 Maßnahmen zum Datenschutz und zur Datensicherheit

Im Prinzip können vier Ebenen der Datenverarbeitung und -kommunikation unterschieden werden:

1. Großrechner (Rechenzentrums-Organisation)
2. Abteilungsrechner (hochleistungsfähige Computer, die - meist ohne eigene Bediener - in der Fachabteilung betrieben werden - oft als Work-Station bezeichnet)
3. Arbeitsplatzrechner (Personal Computer, Laptops)
4. Netzwerke (Zusammenschluss aus PCs und/oder Workstations und/oder Großrechner)

Von der vorhandenen Ebene der Datenverarbeitung hängt es ab, welche konkreten Maßnahmen zum Datenschutz als auch zur Datensicherheit ergriffen werden können. In der Literatur wird vom Ansatz der Maßnahmen her in der Regel zwischen organisatorischen Maßnahmen, baulichen Maßnahmen, hardwaretechnischen, softwaretechnischen und personellen Maßnahmen unterschieden. (Möglich ist auch eine Untergliederung nach der Schutzwürdigkeit der Daten. Vgl. hierzu die Tabelle im Anhang 4-2) Für die Arbeit einer Fachkraft für Arbeitssicherheit sind in der Regel die ersten beiden Datenverarbeitungsebenen (Großrechner, Abteilungsrechner) nicht von Interesse. Meistens haben sie einen eigenen PC und sind vielleicht über das Netz mit anderen Rechnern oder einem Zentralrechner verbunden. Daher werden im folgenden rechenzentrumsspezifische Lösungen vernachlässigt. Es wird bei der Darstellung der einzelnen Maßnahmen davon ausgegangen, dass die Fachkraft für Arbeitssicherheit den Datenschutz im Hinterkopf hat, wenn Arbeitsschutz- oder Datensicherheitsmaßnahmen anfallen.

4.4.1 Organisatorische Maßnahmen

Im Rahmen der organisatorischen Maßnahmen ist zunächst eine Analyse des betrieblichen Datenverarbeitungs-Ist-Zustandes zu erstellen und die zukünftig in diesem Bereich zu erwartenden Veränderungen abzuschätzen. Es werden dabei u.a die eingesetzten Datenträger (Disketten, Laufwerke, CD-Roms u.ä.) registriert, der Ausbildungsstand der mit der Datenverarbeitung beschäftigten Mitarbeiter festgestellt und die bereits vorhandenen Sicherheitseinrichtungen (Zwangssicherungen, Notfallpläne etc.) erfasst. Erst auf diese Weise wird es möglich, Alternativen der Datensicherung zu entwickeln. Außerdem wird so die Grundlage zur Beurteilung einzelner Maßnahmen auf ein Fundament gestellt. /vgl. Gro/ Nach Aleanakian/Kühnau kann die Entwicklung einer Datensicherheitsregelung mit folgenden Stichworten beschrieben werden:

1. Registrierung des Ist-Zustandes
2. Schaffung der Vorraussetzungen für die
3. Schwachstellenanalyse
4. Auswahl von (weiteren) Maßnahmen und deren Einsatz
5. Kontrolle (der Maßnahmen, bzw. deren Einsatz)
6. Falls notwendig, eine Anpassung der Maßnahmen

Die organisatorischen Maßnahmen zur Datensicherung sind hauptsächlich Ablaufhandlungsanweisungen, die ein fehlerloses Funktionieren des Sicherheitssystems ermöglichen und garantieren sollen. Grochla gibt viele Vorschläge, die eigentlich für Rechenzentren gedacht sind, aber auch für PCs oder (lokale) Netze zum großen Teil anwendbar sind:

⇒“Aufstellen eines Organisationsplans
Ein solcher Organisationsplan gibt die fachlichen und disziplinarischen Weisungsbefugnisse zwischen den einzelnen Hierarchiestufen und Abteilungen wieder. Insbesondere interessieren hier die Beziehungen zwischen dem Datenschutzbeauftragten und den mit der Verarbeitung personenbezogener Daten beschäftigten Fachabteilungen. ...

⇒Organisation der Datensicherung bei der Datenübermittlung
In diesem Zusammenhang muss z.B. festgelegt werden, durch wen welche Daten verschlüsselt und übermittelt werden dürfen.

⇒Gestaltung des Arbeitsplatzes und der Arbeitszeit unter Datensicherungsgesichtspunkten
Häufig sind Regelungen für die gleitende Arbeitszeit und den Urlaub der mit Datenverarbeitung beschäftigten Personen sowie für die deshalb erforderliche Übergabe der Arbeitsplätze und Arbeitsunterlagen erforderlich.

⇒Ausarbeitung von Katastrophenplänen
Eine derartige Planung umfasst nicht nur ablauforganisatorische Daten-Sicherungsmaßnahmen wie etwa Evakuierungs- und Benachrichtigungspläne, sondern auch aufbauorganisatorische Datensicherungsmaßnahmen wie Zuständigkeitsregelungen im Falle außergewöhnlicher Gefahr oder die Planung von Ausweich-Kapazitäten.” /Gro/

Grochla hat wie oben schon erwähnt, noch mehr Vorschläge gemacht, die jedoch für Rechenzentren gedacht sind und auf PC oder Netz-Ebene daher etwas grotesk wirken. Es werden noch Vorschläge von Aleanakian/Kühnau /Ale, S. 53 ff./ und Lackmann /Lac, S. 20 ff./ beschrieben, die eigentlich zum Teil so selbstverständlich sind, dass man sie schon wieder betont erwähnen muss:

⇒Sicherungskopien erstellen
Dies ist eine Maßnahme, bei der es eigentlich eine Schande ist, dass sie unter organisatorische Maßnahmen erwähnt werden muss. Wenn jedoch das Sicherungskopienerstellen nicht von `Oben´ angeordnet und kontrolliert wird, ist dies eines der ersten Dinge, die nicht durchgeführt werden. Am besten ist natürlich, wenn es vollautomatisch abläuft, aber dafür war ein PC bzw. die benutzte Software in der Regel nicht eingerichtet – neuere Textverarbeitungsprogramme sind es.

Gehört: Ein neu eingerichtetes Bürosystem versagt seinen Dienst, der Techniker kommt vorbei und repariert es. Dabei gehen wichtige Dateien ins Bitnirwana. Daraufhin fragt er die Sekretärin: "So, das hatten wir. Sie haben doch sicher Sicherungskopien?"
"Ja, da in dem Ordner."
Und da waren sie dann auch, fein säuberliche DIN-A-4-Kopien...
From: Martin.Meyer@p4.f520.n245.z2.fidonet.org (Martin Meyer)

Sicherungskopien werden am besten täglich erstellt. Bei Verlust der Daten ist so maximal eine Tagesarbeit verloren. Aleanakian/Kühnau /Ale, S.54 ff./ und Lackmann /Lac, S. 22/ schlagen mehrere Methoden der Datensicherung vor, welche davon ausgewählt wird, ist gleichgültig; Hauptsache, die Datensicherung wird durchgeführt.

⇒Logbuch führen

Eine nützliche Sache ist ein Logbuch. Für jeden Computer sollten eigene Rubriken vorgesehen werden. Eingetragen werden Anschaffungsdatum, Reparaturen, Software (-installationen, z.B. Updates), geplante und durchgeführte Checks und besondere Vorkommnisse.

⇒Notplan erstellen

Dies kann natürlich nicht für jeden möglichen Fehler erstellt werden, aber die (un-) geplante Abwesenheit des zuständigen Mitarbeiters soll nicht den Stillstand des Systems zur Folge haben. "Wichtige Informationen, die ein Notplan enthalten muss, sind

◊ die Telefonnummern der Personen, die in bestimmten Situationen helfen können, wie zum Beispiel die Rufnummer des Hardware-Technikers,
◊ eine Hardware-Wiederbeschaffungsliste,
◊ Aufbewahrungsorte der Disketten,
◊ Aufbewahrungsorte aller wichtigen Unterlagen im Zusammenhang mit der EDV." /Ale, S.62/

⇒Wartungsverträge abschließen

Insbesondere in Betrieben, in denen kein Computerfachmann vorhanden ist, empfiehlt es sich, einen Wartungsvertrag abzuschließen. Dies ist nicht gerade billig, kann sich aber schon bei Auftreten eines einzigen entsprechenden Schadenfalles rechnen. Am besten ist es, einen Vertrag für die ganze Hardware abzuschließen, z.B. um Kompetenzstreit zu vermeiden. Ebenso sollte die Software über solche Verträge abgesichert werden; in der Regel beinhalten solche Verträge den Vorteil, dass man die jeweils neueste Version des Programms zur Verfügung hat.

⇒Versicherungsschutz

Eine letzte Möglichkeit, die noch vorgeschlagen werden soll, ist der Abschluss von Versicherungen. Ob sich Versicherungen rechnen, muss man für jeden Einzelfall kalkulieren. Es gibt auf dem Markt verschiedene Arten passender Versicherungen, z.B. können im Bereich EDV-Verarbeitung u.a. folgende Versicherungen abgeschlossen werden:

◊ Neuwert-/Zeitwertversicherung
◊ Datenträgerversicherung
◊ Datenschutzhaftpflichtversicherung

◊ Maschinen-/Betriebsunterbrechungsversicherung

◊ Mehrkostenversicherung

◊ Missbrauchsversicherung

◊ Vertrauensschadenversicherung und die gewöhnliche

◊ Haftpflichtversicherung /vgl. Ale, S. 68/

4.4.2 Bauliche Maßnahmen

Viele dieser Maßnahmen, die in der Literatur (z.B. Grochla) vorgeschlagen werden, werden beim Einsatz von PCs oder lokalen Netzen als nicht notwendig betrachtet. Es werden trotzdem viele dieser Maßnahmen aufgezählt, denn selbst wenn man sie nicht wegen der Rechner in Erwägung zieht, sind diese Maßnahmen aus ergonomischen Überlegungen oder anderen Sicherheits-Überlegungen (z.B. Feuerschutz, Einbruch und Diebstahl) interessant:

⇒ elektrische Leitungen neu verlegen

⇒ Installation von Notstromaggregaten

⇒ Trenn- und Zwischenwände einziehen, bzw. Abreißen

⇒ feuerfeste Stahltüren anschaffen

⇒ Installation von Feuermeldern und Feuerlöschanlagen

⇒ Klimaanlage einbauen

⇒ Automatische Türen anschaffen oder

⇒ Türen mit Schnappschlössern einbauen

⇒ vorhandene Türschlösser durch verlängerte Winkeleisen verstärken

⇒ Türrahmen und Türblätter durch zusätzliche Verstärkungen absichern

⇒ Fenstergriffe und Rollladen einbauen, die fest mit dem Mauerwerk verbunden sind

Diese Maßnahmen sollten mittlerweile auch beim Einsatz eines PC (Stand-Alone oder als lokales Netz) in Erwägung gezogen werden, denn aufgrund der schnellen technischen Entwicklung werden gerade auf diesen Rechnertypen immer höhere Datenmengen verarbeitet und abgespeichert. Aber diese Vorschläge sind mit den Argumenten: `PC-Einsatz, Datensicherheit/-schutz´ alleine kaum durchzusetzen; doch ein großer Teil der Vorschläge ist z.B. unter allgemeinen Feuerschutzgedanken ebenfalls notwendiger Bestandteil eines Maßnahmenkataloges.

4.4.3 Hardwaretechnische Maßnahmen

Hardwaretechnische Maßnahmen umfassen die stromversorgenden Teile des Rechners sowie die im Rechner selbst integrierten mechanischen oder sonstigen Schutzeinrichtungen. Grochla versteht darunter auch sonstige maschinellen Anlagen oder Einrichtungen im Zusammenhang mit EDV-Anlagen. Er gibt hier einige Beispiele, die direkt für Rechenzentren einsetzbar sind, aber auch für den PC-Einsatz im großen und ganzen ohne wesentliche Änderungen geeignet sind:

⇒"Schlüsselschalter und Terminschalter
Es handelt sich hier um physische Identifikationsmerkmale, die nur dem Besitzer den Zugang zur ADV-Anlage erlauben. Der Nachteil einer solchen Sicherungseinrichtung ist der, dass auch Unbefugte in den Besitz des/der Schlüssel gelangen können, da das Identifikationsmerkmal `Schlüssel´ unabhängig von der nutzenden Person ist." /Gro/ Dass die für PCs angebotenen Einrichtungen nicht gerade den technisch höchsten Stand haben, sollte nicht daran hindern, sie zu nutzen. Gelegenheitshacker sind damit vielleicht doch abzuschrecken.

⇒"Schreib- und Lesesicherungen
Durch aufklebbare Markierungen an Disketten oder Magnetbandleseringe soll die zufällige Zerstörung gespeicherter Daten und Programme durch eine Fehlbedienung der Anlage verhindert werden." /Gro/ Eine saubere Beschriftung der Disketten und Magnetbänder ist zusätzlich empfehlenswert und auch aus Ordnungsgründen nützlich. Die neueren Disketten haben als Lösch- bzw. Schreibschutz herausbrechbare bzw. schiebbare Laschen.

⇒"Feuerfeste Stahlschränke und verschließbare Datenträger-Container
Diese Datensicherungsmaßnahmen dienen der ordnungsgemäßen Aufbewahrung und dem ordnungsgemäßen Transport der Datenträger.

⇒Anlagen zur Vernichtung von Datenträgern
Soweit nicht mehr benötigte Daten nicht durch einfaches Löschen und Überspeichern des Datenträgers gelöscht werden können, müssen sie gemeinsam mit dem jeweiligen Datenträger vernichtet werden. Reißwolf- oder Verbrennungsanlagen sind hierfür geeignete hardwaretechnische Einrichtungen." /Gro/ Es gibt Unternehmen, welche die Vernichtung von Aktenmaterial, Datenbanken u. ä. nach BDSG (bzw. dessen Anforderungen) schnell, problemlos und kostengünstig durchführen.

⇒Sichere und zuverlässige Stromversorgung
Spätestens wenn der Rechner auch nur für ein paar Sekunden ausgefallen ist, und die Arbeit von mehreren Stunden umsonst war, nimmt man die Stromversorgung wahr. Für Rechenzentren sind daher unterbrechungsfreie Stromversorgungen üblich. Bei PC-Anwendern ist es halt eine Geldfrage, ob man 4 000,- DM für eine batteriegestützte unterbrechungsfreie Stromversorgung ausgeben kann und/oder will.

Aber schon Stromschwankungen können gefährlich sein. Netzfilter, Störschutztransformatoren und magnetische Spannungskonstanthalter steigern die Zuverlässigkeit des Gerätes. Sie sind oft schon eingebaut, anderenfalls liegen die Kosten für den Einbau solcher Geräte bei einigen hundert DM.

⇒Maßnahmen gegen elektrostatische Entladungen

Elektrostatische Entladungen können zu Schäden am Computer führen (tritt sehr selten auf, trifft meistens die Tastatur), sie führen oft jedoch zu Programmfehlern, d.h. zu sonderbaren Reaktionen des Programms und damit möglicherweise zu Datenverlusten. Daher sollte man auch so etwas vermeiden. Dazu schlagen Aleanakian/Kühnau folgende Maßnahmen vor, die sie in zwei Gruppen aufteilen:

1. Vermeidung einer Aufladung mit folgenden Maßnahmen:
◊ "Erhöhung der relativen Luftfeuchtigkeit ...,
◊ Verlegung antistatischer oder Verzicht auf Teppichböden,
◊ Vermeidung von Kleidung aus Kunstfasern und von Schuhen mit Kunststoff- oder Gummisohlen." /Ale, S. 90/91/
2. Bereits entstandene Aufladungen ableiten mittels:
◊ "leitfähiger Bürostühle,
◊ Schreibtische und
◊ Arbeitsunterlagen für den Computer." /Ale, S.92/

Computer sind selbstverständlich zu erden wie auch die verschiedenen anderen elektrischen Geräte in der Regel geerdet werden. In der Regel reicht ein Teil der Maßnahmen als Schutz aus.

⇒Schutz gegen elektromagnetische Störstrahlung

Dies ist ein Spezialgebiet, auf dem auch Fachleute Probleme haben, diesen Fehler und die Fehlerquelle entdecken und zu beseitigen. Es wird nur der Vollständigkeit wegen erwähnt. Hierbei handelt es sich um hoch-frequente elektromagnetische Felder, die sich z.B. auf ungenügend abgeschirmte Datenleitungen auswirken. Erzeuger solcher Strahlung sind:

◊ "Funkgeräte oder -anlagen
◊ medizinische Geräte, die mittels Hochfrequenz Wärme erzeugen,
◊ bestimmte Schweißgeräte
◊ Leuchtstoffröhren
◊ Mikrowellenherde und
◊ starke elektrisch geregelte Antriebe.

...

Im übrigen ist auch der Personalcomputer eine mögliche Störquelle für andere Geräte, wie Radio- und Fernsehempfänger." /Ale, S.92/93/

4.4.4 Softwaretechnische Maßnahmen

Theoretisch können softwaretechnische Maßnahmen wie folgt definiert werden: "Unter softwaretechnischen Maßnahmen sind alle in Betriebs- und Anwendungsprogrammsystemen implementierten Sicherungsmaßnahmen zu verstehen. Hard- und Software sind dabei nicht unabhängig voneinander, sondern müssen sinnvoll kombiniert werden, um eine wirkungsvolle Datensicherung zu erreichen.
Beispiele für softwaretechnische Datensicherungsmaßnahmen, die sowohl BDSG-initiiert sein können, als auch auf unternehmenseigenen Interesse beruhen können, sind:

⇒Softwaretechnischer Schutz vor unbeabsichtigtem oder unbefugten Eingeben, Lesen, Kopieren oder Löschen von Daten
Derartige Datensicherungsmaßnahmen können grundsätzlich für alle maschinell zu verarbeitenden Daten eingeführt werden. Unter Berücksichtigung des Verhältnismäßigkeitsprinzips ist im konkreten Einzelfall zu klären, in welchem Umfang neben der schon vorhandenen hardwaretechnischen Sicherung (Tastaturschlösser etc.) softwaretechnische Datensicherungsmaßnahmen eingeführt werden müssen.

⇒Festlegung eines Algorithmussees zur Überprüfung der Nutzungsberechtigung mit Hilfe von Paßwörtern, Zahlenkombinationen etc.
Die Vorteile derartiger Erkennungsvorgänge liegen in ihrer einfachen Realisierbarkeit und ihren hohen Sicherheitsniveau. Es ist jedoch sicher zustellen, dass mögliche Listen mit Paßwörtern nicht von Unbefugten eingesehen werden können und die Eingabe verdeckt erfolgen kann." /Gro/

Die aus dem Großrechnerbereich stammenden Maßnahmen wie Paßwortschutz für das Gesamtsystem als auch für einzelne Anwendungsprogramme (unterteilt in Lese, Schreib und Überschreibrechte) sind mittlerweile auch am PC nicht nur möglich und werden auch von der Industrie angeboten, sondern sind auch notwendig - insbesondere, wenn er an ein Computernetz angeschlossen ist. Denn die Datenmengen und auch die Datenvielfalt eines PC haben mittlerweile enorme Ausmaße angenommen und häufig werden personenbezogene oder nicht für die Öffentlichkeit geeignete oder bestimmte Daten gespeichert. Paßwörter werden auch bei PCs auf verschiedenen Ebenen benutzt:

◊ "beim Systemstart direkt nach dem Einschalten,
◊ vor Benutzung von Anwendungsprogrammen,
◊ beim Aufruf bestimmter Funktionen innerhalb eines Programms (zum Beispiel Löschbefehle)

◊ beim Zugriff auf bestimmte Daten aus den Anwendungsprogrammen heraus (zum Beispiel Kundendatei)." /Ale, S. 78/

⇒Festlegung der Nutzungszeit

Grochla schlägt noch eine weitere Maßnahme vor, die im Großrechnerbereich häufig angewendet wird: das Festlegen einer Nutzungszeit (Timed log-in; Timed log-out). Für den PC-Bereich gibt es einzelne Programme, die so etwas oder ähnliches anbieten, aber der Nutzen ist doch sehr umstritten.

⇒Automatische Protokolle

Auch diese Maßnahme kommt aus dem Großrechnerbereich. Im Gegensatz zur letztgenannten Maßnahme setzt sich diese Maßnahme insbesondere bei Netzen durch, da hier doch einige Vorteile zu sehen sind. Aleanakian/Kühnau wollen

◊ "Hardwarestörungen, sofern sie nicht zum Totalausfall des Rechners führen,
◊ Programmabbrüche
◊ Aufruf bestimmter Anwendungen sowie
◊ Änderungen am Datenbestand" /Ale, S.82/

protokolliert haben. In PC-Netzen werden oft letzte Log-in Zeit, letzte Log-out Zeit, die Anzahl der Log-in Versuche, die aufgerufenen Programme und die Störungen im System erfasst. Um bei Ausfall des Rechners verfügbar zu sein, sollten diese Informationen so häufig wie möglich ausgedruckt werden oder Sicherungskopien erstellt werden. Ein ähnliches (Software-) Prinzip wird mittlerweile bei den meisten Anwendungsprogrammen angewendet, um vier oder fünf Arbeitsschritte zu speichern.

⇒Automatische Datenprüfung

Die Datenprüfung kann (und sollte auch) gleich bei der Eingabe erfolgen. In der Regel werden hier formaler Aufbau und Plausibilität der Daten nachgeprüft. Anwendungssoftware sollte auch danach beurteilt werden, welche Prüfmöglichkeiten sie vorsehen. Aber auch danach sollten Daten unter folgenden Gesichtspunkten automatisch überprüft werden:

◊ Menge der Datensätze in einer Datei,
◊ Aufbau der Datensätze einer Datei,
◊ Gesamtmenge der Daten (Anzahl und Größe der Dateien),

um z.B. Fehler in der Dateiverwaltung zu entdecken. Es gibt hierzu eigene Prüfprogramme, die Fehler in der Dateiverwaltung entdecken können. D.h. falls das Rechnerbetriebssystem solche Kontrollen nicht vorgesehen hat, sollten solche Prüfprogramme angeschafft werden.

⇒Verschlüsselung von Daten

Gerade bei der Speicherung personenbezogener Daten ist eine Verschlüsselung aus Datenschutzgründen sehr empfehlenswert. Aber auch bei anderen Daten, die nicht für die Öffentlichkeit bestimmt sind, ist die

Verschlüsselung ein geeignetes Datensicherungsmittel. Es gibt auch mittlerweile für den PC-Bereich Software, die Daten nur verschlüsselt abspeichert. Ein weiterer Anwendungsfall ist der Bereich der Datenübermittlung. Eine Verschlüsselung der Daten ist hier ebenfalls notwendig, denn es ist kein Problem Daten auf dem Leitungsweg einzusehen. Der Empfänger muss selbstverständlich über die entsprechenden Entschlüsselungscodes oder entsprechende Software verfügen.

Die oben aufgeführten softwaretechnischen Maßnahmen können als vorbeugende (ex-ante Maßnahmen, sollen Datenmissbrauch verhindern) und aufklärende (ex-post Maßnahmen, sollen das Aufdecken eines unberechtigten Zugriffs ermöglichen) Maßnahmen unterschieden werden. Aufklärende Maßnahmen erfüllen jedoch nur dann ihren Zweck, wenn die Protokolle oder sonstigen Aufzeichnungen regelmäßig überprüft und ausgewertet werden.

4.4.5 Personelle Maßnahmen

Diese Maßnahmen werden in der Regel unter organisatorischen Maßnahmen geführt, bekommen hier jedoch ihrer Bedeutung entsprechend in Anlehnung an Grochla einen eigenen Abschnitt. Denn vom Mensch verursachte Fehler - sei es nun bewusst oder unbewusst - können als die größte Fehlerquelle bei der Datenverarbeitung angesehen werden. Man kann es ruhig so formulieren:

Der Mensch ist der größte Schwachpunkt im Datensicherungssystem!

Daher müssen Personalmaßnahmen ergriffen werden, und diese fangen schon bei der Personalplanung an, gehen über die Personalauswahl hinaus notfalls bis zur Personalüberwachung. Auch das Bundesdatenschutzgesetz fordert personelle Maßnahmen, z.B. muss ein Datenschutzbeauftragter bestellt werden und die Mitarbeiter müssen auf das Datengeheimnis verpflichtet werden. Insbesondere in diesem Bereich sind Datenschutz und Datensicherheit sehr eng verzahnt, wie die folgenden Beispiele von Grochla (ähnliches Beispiele haben auch Jaburek /Jab/, Lackmann /Lac/ und Aleanakian/Kühnau /Ale/ etc.) zeigen:

⇒"Auswahl der Mitarbeiter des DV-Bereiches unter Zugrundelegung der persönlichen und fachlichen Stellenanforderungsprofile
Hierbei sollte der bisherigen Tätigkeit der Bewerber besondere Aufmerksamkeit geschenkt werden. Vor allem ist zu prüfen, ob bei Ihnen Unregelmäßigkeiten im Bereich der Datenverarbeitung vorgekommen sind." /Gro/ Hier ist es besser zu schreiben: bekannt sind und dieses Wissen weitergegeben wird. Grochla legt viel Wert auf die grundsätzliche Einstellung des Bewerbers zum Datenschutz, aber gerade in diesem Bereich kann man im Vorstellungsgespräch viel erzählen. Unseres Erachtens ist wichtig, dass sich der Bewerber der Datensicherheit- und der Datenschutzproblematik bewusst ist.

⇒Durchführung von Mitarbeiterschulungen
Die Mitarbeiterschulungen können rein aus Datenschutzgründen durchgeführt werden. Sie dienen der Erhaltung eines aktuellen Wissenstandes der Mitarbeiter in Datenschutzbelangen; diese Schulungen sind nach Grochla Hauptaufgaben der Unternehmung. /vgl. Gro/ In der Regel werden Schulungen aus Datensicherheitsgründen durchgeführt, dies oft anlässlich der Einführung einer neuen Release eines (Anwendungs-) Programms. So spart das Unternehmen Geld und erfüllt trotzdem seine gesetzlichen Verpflichtungen.

⇒"Kontrolle der Mitarbeiter
Die Kontrolle der Mitarbeiter - auch in Fragen des Datenschutzes - wird sowohl direkt durch das BDSG gefordert, als auch aus unternehmenseigenem Interesse durchgeführt. Hierbei lässt sich die Kontrolle zum einen stellengebunden und zum anderen personengebunden durchführen. Im Regelfall wird eine stellengebundene, oftmals nur stichprobenartig durchgeführte Kontrolle genügen, während vor allem im Verdachtsfall personengebundene Kontrolle durchgeführt werden sollen. Derartige Kontrollen können sowohl Sichtkontrollen als auch automatische Kontrollen sein. Die jeweilige Vorgehensweise bestimmt sich hierbei nach den betrieblichen Gegebenheiten." /Gro/ Um Missverständnisse zu vermeiden: hier geht es um die Weitergabe nicht für die Öffentlichkeit bestimmter Daten, seien es nun Daten, die unter das Bundesdatenschutzgesetz fallen oder Daten, die aus anderen Gründen nur betriebsintern gehandhabt werden dürfen. Dieses Problem kann auch in einem kleinen Betrieb mit wenigen Mitarbeitern anfallen. Es geht nicht um eine Leistungskontrolle oder um die Kontrolle privater Dinge.

⇒Beendigung von Arbeitsverhältnissen
Dies ist so ein Fall, wo man auf den guten Willen der (ehemaligen) Mitarbeiter angewiesen ist, denn die Loyalitätsverpflichtung zum (ehe-

Und jetzt noch, nachdem man sich so schön über andere lustig gemacht hat, ein echter Oberknaller, der mir selbst passiert ist:
Nach der Arbeit hatte ich noch für eine Messe was vorzubereiten und habe ein 88er Syquest-Laufwerk mit nach Hause genommen, um auch die Daten verfügbar zu haben. Außerdem hatte ich noch eine Menge anderen Kram dabei und stellte, um alles einzuräumen, das Syquest-Laufwerk "zunächst" auf das Dach meines Autos. Als ich dann auf der Autobahn war, fährt plötzlich so ein "Spinner" neben mir, der immer nach oben zeigt. Ich verstehe Bahnhof und er gibt mir zu erkennen, dass ich auf den Seitenstreifen fahren soll. Ich fahre auf den Seitenstreifen, der Typ hält hinter mir, steigt aus und kommt nach vorne. Ich kurble das Fenster runter und noch bevor ich fragen kann, nimmt er das Syquest vom Dach und reicht es mir obercool zum Fenster rein, ohne irgendwas zu sagen ...
From: Frank Renner, frank.renner@castrop-rauxel.netsurf.de

maligen) Arbeitgeber ist ja quasi mit dem Ende des Arbeitsverhältnisses erloschen. So kann ein großes Problem mit der Beendigung eines Arbeitsverhältnisses entstehen, insbesondere wenn der Mitarbeiter nicht im Guten geht. Der ausscheidende Mitarbeiter kann natürlich verpflichtet werden, betriebsbezogene Kenntnisse nicht missbräuchlich zu verwenden. Ob er diese Verpflichtung ernst nimmt, ist eine andere Frage. Jeder kennt zwar den Spruch: `Man liebt den Verrat, aber nicht den Verräter.´ Dies interessiert aber einen (im Bösen gegangenen ehemaligen) Mitarbeiter manchmal nicht, insbesondere wenn der Verrat entsprechend gut honoriert wird. Man kann aber wenigstens Authentifikationsschlüssel (z.B. Paßwort), Chiffrierungs- und Dechiffrierungscodes ändern, um zu vermeiden, dass (über Netz) Unbefugte in den Rechner eindringen.

4.5 Betriebswirtschaftlicher Nutzen des Datenschutzes

Die bisher beschriebenen Punkte waren die Aspekte des Datenschutzes, die Kosten verursachen. Außer dass Datenschutz in der Regel auch der Datensicherheit dient, können ebenso andere Nutzeffekte auftreten. Bei den folgenden beschriebenen nützlichen Auswirkungen handelt es sich um betriebswirtschaftliche, also um unternehmensbezogene Auswirkungen. Der gesellschaftliche, politische oder juristische Nutzen wird hier nicht beschrieben, um nicht zu sehr ins politische und juristische abzudriften. Grochla hat eine Zusammenfassung der betriebswirtschaftlich interessanten Nutzwirkungen geschrieben, die als Überblick vollkommen ausreichend ist:
“Diese betrieblichen Nutzenaspekte können unterschieden werden in

◊ Nutzen, die bei der betrieblichen Datenverarbeitung entstehen,
◊ Nutzen, die sich für die Mitarbeiter ergeben, und
◊ Nutzen, die im Kontakt zu Lieferanten und Kunden wirksam werden.

Für die betriebliche Datenverarbeitung können durch die Vorschriften des BDSG unter Umständen folgende positive Effekte entstehen:

⇒ Die Überprüfung, welche Vorschriften des BDSG für die jeweilige Unternehmung relevant sind, sowie insbesondere die Überlegungen, wie die einzelnen vom BDSG auferlegten Verpflichtungen erfüllt werden können, werden häufig der Anlass für eine grundsätzliche Überprüfung der Ablauforganisation innerhalb der betrieblichen Datenverarbeitung sein. Bei dieser Überprüfung können eventuelle Schwachstellen erkannt und beseitigt werden.
⇒ Die Datenverarbeitung wird auf Grund einer übersichtlicheren Organisation der Datenbestände oder einer klareren Aufgabenzuweisung unter Umständen rationeller durchgeführt.

⇒Durch zusätzliche Schutzmaßnahmen, die BDSG-relevante Störungen oder Ausfälle im Verarbeitungsprozess ausschließen sollen, kann die Datenverarbeitung ferner zuverlässiger werden.

⇒Durch eine systematischere Struktur kann die Qualität der Datenverarbeitungsergebnisse, also der Daten und Dateien, verbessert werden.

⇒Redundanzen innerhalb der Datenverarbeitung, z.B. die mehrfache Führung derselben Datei an verschiedenen Stellen, können aufgedeckt und vermindert werden.

⇒Die Notwendigkeit einer vollständigeren und zeitnäheren Dokumentation kann deutlich werden, wodurch auch eine bessere Prüfung aller Vorgänge möglich wird.

⇒Unternehmensinterne Regelungen für die Datenübermittlung und die übrigen Phasen der Datenverarbeitung können angeregt werden.

⇒Die Erstellung oder Verbesserung einer Übersicht über alle vorhandenen Sicherungsmaßnahmen sowie die Abstimmung der Maßnahmen untereinander werden überprüft. Darüber hinaus kann auf diese Weise leichter kontrolliert werden, ob die Anforderungen des BDSG hinreichend erfüllt sind.

⇒Eine Verbesserung der Datensicherung im unternehmenseigenen Interesse, etwa der Schutz nicht-personenbezogener Daten, kann erreicht werden. So können beispielsweise für den Schutz nicht-personen-bezogener Geschäftsdaten unternehmensintern die gleichen oder ähnliche Richtlinien erlassen werden, wie für personenbezogene Daten im BDSG festgelegt sind. /Gro/

Die folgenden Gründe, für die ebenfalls Grochla zitiert wird, sind mittlerweile fast antiquiert, werden aber trotzdem beschrieben, denn das Thema `Datenschutz´ ist immer noch wichtig, wenn es auch durch das Thema `Datensicherheit´ etwas in den Hintergrund gedrängt wurde und im Alltagsgeschehen daher wieder mehr in den Vordergrund rücken sollte. Insbesondere die von Grochla erwähnte öffentliche Diskussion ist eingeschlafen, da andere Themen aus diesem Bereich wichtiger erscheinen. Speziell die Virenproblematik hat das Thema Datenschutz in der Diskussion der Anwender verdrängt und spielt im Bereich Datensicherheit schon seit mehreren Jahren eine große Rolle. Dieses Problem wird deshalb auch in einem eigenem Kapitel extra behandelt.

Grochla sieht neben den schon genannten positiven Auswirkungen des Bundesdatenschutzgesetzes auch Nutzenaspekte für die Mitarbeiter eines Unternehmens und den positiven Einfluss des Gesetzes auf deren Handlungen im Bereich der betrieblichen Datenverarbeitung:

⇒"Allgemein wurden und werden die Mitarbeiter durch die öffentliche Diskussion der Datenschutzthematik für Fragen des Datenschutzes und der Datensicherung sensibilisiert und stehen der Problematik aufgeschlossener gegenüber als vorher. Das Sicherheitsbewusstsein der Mitarbeiter wurde auf diese Weise erhöht, so dass sie von sich aus auf grobe Datenschutzverfehlungen in ihrem Bereich achten.

⇒Bei vielen Mitarbeitern wurde ein gesteigertes Bewusstsein für die Belange der Betroffenen geweckt. Sie unterlassen daher häufig Speicherungen, Übermittlungen und sonstige Verarbeitungen, deren Zulässigkeit ihnen fraglich erscheint, oder konsultieren zunächst den Datenschutzbeauftragten. Die Unternehmensleitung kann so auf unerlaubte Verarbeitungen hingewiesen werden und diese unterlassen oder ändern.

⇒Durch das gestiegene Datenbewusstsein kann bei den Mitarbeitern eher mit Verständnis für die Durchführung erforderlicher Datenschutz- und Datensicherungsmaßnahmen gerechnet werden. Mit Hinweis auf die Anforderungen des BDSG können daher auch unbequeme oder aufwendige Maßnahmen leichter durchgesetzt werden. Die Akzeptanzprobleme können verringert werden.

⇒Das Vertrauen der Mitarbeiter und des Betriebsrates in die Ordnungsmäßigkeit der Datenverarbeitung, insbesondere soweit sie die Verarbeitung personenbezogener Daten der Mitarbeiter betrifft, kann gestützt werden. Sehen die Mitarbeiter, dass die Unternehmung bei der Datenverarbeitung verantwortungsbewusst und dem BDSG gemäß vorgeht, kann ein häufig vorhandenes Misstrauen gegen die Verarbeitung personenbezogener Daten der Mitarbeiter zumindest teilweise abgebaut werden. Auf diese Weise kann es in diesem Bereich zu einem verbesserten Verhältnis zwischen der Unternehmungsleitung einerseits sowie den Mitarbeitern und Betriebsrat andererseits kommen." /Gro/

Die von Grochla übernommenen Gründe erscheinen und sind wohl auch in vielen (Groß-) Unternehmen längst überholt, aber gerade bei kleinen und mittleren Unternehmen sollte eine Fachkraft für Arbeitssicherheit mal bei den Kollegen schauen, wie es im Verhältnis zum Datenschutz steht. Denn wer sich um den Datenschutz nicht kümmert, vernachlässigt in der Regel auch die Datensicherheit. Aber gerade diese ist für kleine Unternehmen sehr wichtig und oft bedeutsam im Verhältnis zu Kunden und Lieferanten. Wenn hier infolge schlechter Datensicherung ein Auftrag verpatzt wird und der Kunde verloren geht, kann das für das Unternehmen ruinöse Folgen haben. Grochla schreibt hierzu:

⇒"Im Verhältnis sowohl zu Kunden als auch zu Lieferanten wird, ähnlich wie im Verhältnis zu den Mitarbeitern, eine vertrauensvollere Zusammenarbeit möglich, wenn bekannt ist, dass die Unternehmung mit allen bei ihr

gespeicherten Daten verantwortungsbewusst und im Sinne des BDSG umgeht. Insbesondere bei geheimen oder zumindest nicht für die breite Öffentlichkeit bestimmten Daten werden die Geschäftspartner Wert auf die Gewissheit legen, dass diese Daten bei der Unternehmung ordnungsgemäß verarbeitet und gespeichert werden und nicht von jedermann abgefragt oder sogar verfälscht werden können. Dies gilt selbstverständlich nicht nur für personenbezogene, sondern auch für nicht-personenbezogene Daten." /Gro/

Grochla bemerkt noch, dass verschiedene Unternehmen wie Banken, Versicherungen und Versandhäuser, durchgeführte Datenschutzmaßnahmen für Öffentlichkeitsarbeitszwecke verwenden könnten, um so ein bestimmtes Image aufzubauen. Dies wird in den letzten Jahren kaum gemacht, da es gerade in diesen Branchen so gut wie keine Unternehmen gibt, die nicht nach dem Datenschutzgesetz arbeiten.

Grochlas Aufzählung möglicher Nutzenaspekte des Bundesdatenschutzgesetzes kann nach seinen Worten keinen Anspruch auf Vollständigkeit erheben. Sie bietet aber einen schönen Überblick darüber, dass die Unternehmen durch dieses Gesetz nicht nur Kosten haben, sondern auch Vorteile. Der Nachteil dieser Vorteile ist jedoch, dass sie sich nur schwer oder gar nicht in Geldwert beziffern lassen. Die beschriebenen Nutzen sind fast nur immaterieller Art und können daher schlecht mit den hierfür notwendigen Kosten verglichen werden. Viele Forderungen des Bundesdatenschutzgesetzes sind jedoch auch unter dem Stichwort Datensicherheit führbar und wären daher aus unternehmenseigenem Interesse sowieso durchgeführt worden. Ihre Kosten sollten deshalb den Kosten für Datenschutzmaßnahmen nicht zugeschlagen werden.

Noch mehr Informationen zum Thema Datenschutz und Datensicherheit findet man im Anhang und in der angegebenen Literatur im Literaturverzeichnis.

Zum Abschluss des Kapitels noch eine zweideutige Geschichte (für die Betroffenen war sie nicht so lustig wie sie sich liest) zu den Grenzbereichen des Datenschutzes:

« Folgende Kurzinfo über die neuen Praktiken der Finanzämter erreichte uns kürzlich über e-mail:

Im Vorfeld von Betriebsprüfungen haben Mitarbeiter der Finanzämter sich u.a. bei einer Niederlassung eines namhaften Automobilherstellers über die km-Stände der verschiedenen Taxibetriebe informiert. Die Niederlassung war so hilfsbereit, die gewünschten Angaben problemlos zu liefern.

O-ton: "wir haben uns nichts dabei gedacht."

Dies führte dann im Ergebnis zu deutlichen Zuschätzungen bei den Umsätzen mit den entsprechenden Folgen.

Euer Würfelfunk   Berlin, den 10.05.96»

5 Computerviren

Es sind inzwischen mehr als 3000 DOS-Viren bekannt. Davon sind in Deutschland ca. 30 Stück stärker verbreitet. Es steht jedoch außer der üblichen Übertragungsmöglichkeit (graue Software, nicht lizenzierte Spiele usw.) den Virenschöpfern auch immer mehr das Internet zur Verfügung (die Anschlusszahlen am Internet steigen stetig, denn die Vorteile des Internet sind immens). Daher sind die genannten Zahlen nur Anhaltswerte, sie können sich täglich ändern. Ein heute noch unbekannter Virus kann z.B. durch das Internet ganz schnell verbreitet werden und in die sogenannte Viren-Spitzengruppe aufrücken. Ein Problem ist, dass die Virenproduzenten immer raffinierter werden und daher bislang ausreichende Schutzmaßnahmen doch oft nicht mehr genügen und von den Viren umgangen werden. /so schon 1993 Langemeyer, Lan/
Ursprünglich sollte im Anhang eine Teilliste bekannter Viren zu finden sein. (Amerikanische) Unternehmen, die z.B. auch von der Virenbekämpfung leben, veröffentlichen so etwas u.a. im Internet. Diese Listen werden (wie wohl auch von den Lesern erwartet) mit den Hinweisen versehen, dass sich der Inhalt dauernd ändern kann und dass sie nicht vollständig sein können. Die Autoren haben selbst beobachtet, wie sich so eine Liste innerhalb eines Jahres geändert hat und begnügen sich daher auf den Hinweis, dass z.B. im Internet solche Listen zu finden sind. Ähnliches gilt für die Antivirensoftware; hier soll auf die Arbeiten von Stang /ICS/ und Slade /Sla/ verwiesen werden.
Viele werden sich noch an den Medienrummel um den Michelangelo-Virus 1992 erinnern. Hier zeigte sich wieder mal, \`dass nichts so heiß gegessen wird wie es gekocht wird´ - die angekündigte Katastrophe blieb aus. Das Problem \`Computervirus´ wurde jedoch in der breiten Öffentlichkeit bekannt. Viele Rechner wurden gerade in dieser Zeitspanne auf Viren durchsucht und so mancher Virus wurde auch gefunden. Mittlerweile ist dieses Thema der Presse keine Schlagzeile mehr wert - obwohl es mehr Viren gibt, die z.T. noch gefährlicher sind und die Situation nach Michelangelo keinesfalls als entspannt bezeichnet werden kann. /vgl. Lan/ Dies sollen folgende allgemeine Beispiele zeigen:

Der Vir in uns

Nach Angaben der britischen Regierung ist die größte Sicherheit vor der Rinderseuche BSE durch einen Internetanschluss zu erreichen. Wie es hieß, seien da nicht nur die Übertragungsraten extrem niedrig, teilweise breche die Übertragung sogar ganz zusammen.
von Ulrich Horb (uho) in zitty 11/96

Es gibt Viren, die ihren Code verändern. Damit erschweren sie ihre Erkennung sehr. Sie werden als mutierender Virus bezeichnet. Andere Viren (Bezeichnung ist Tarnkappenvirus) modifizieren das Betriebssystem, d.h. passen dies ihren Bedürfnissen an. Wieder andere Viren vermehren sich nur ereignisgesteuert. Sie werden also auf den sogenannten `Quarantäne-Stationen´ nicht entdeckt. /vgl. Lan S. 48, Slade und insbesondere Stang behandeln einzelne Virentypen und ihre Wirkung ausführlich, Sla, S. 47 ff., ICS, S. 53 ff./

Viele Gerüchte behaupten immer wieder, dass die Softwareindustrie selbst Viren produziert, um z.B. Anti-Viren-Produkte verkaufen zu können. Dies werden die Firmen jedoch gar nicht nötig haben, denn es gibt genügend andere Gruppen, die Viren herstellen. Langemeyer hat einige Typen mitsamt den möglichen Beweggründen aufgezählt:

⇒ "Der Zauberlehrling = Ein Junginformatiker, der das Virenphänomen selbst untersuchen möchte, aber aus Unachtsamkeit fahrlässig infizierte Programme weitergibt. (keine kriminelle Absicht!)

⇒Der `Robin Hood´ = Ein Ideologe, der den gläsernen Menschen verhindern will, indem er den Computer-anwender verunsichert.

⇒Der Vandalist = Ein DV-Spezialist, der seinen Frust ab-bauen will oder Spaß am Zerstören hat.

⇒Das `Rumpelstilzchen´ = Ein DV-Spezialist, der im Verborgenen sich freut, welchen Schaden sein besonders raffiniert arbeitender Virus anrichtet.

⇒Der Saboteur = Ein Mitarbeiter einer Firma, der der Kon-kurrenz schaden möchte." /Lan, S. 52/

Als erste Gruppe erwähnt Langemeyer das Militär. Dies ist wohl auch die wichtigste Gruppe. In den USA wird die Virenforschung und -erstellung stark vom Pentagon gefördert. Insbesondere Viren gegen Waffensysteme werden entwickelt. Es wird vorerst nicht bewiesen werden, aber im Golfkrieg wurden wohl Computerviren eingesetzt. Langemeyer bezeichnet solch ein Vorgehen als problematisch. Dies ist vorsichtig formuliert, den dies ist eine Methode, die leicht außer Kontrolle geraten kann.

In der Firma, in der ich vor ein paar Jahren gearbeitet habe, hat ein 'Viren-Guru' (den Namen habe ich leider vergessen) einen Vortrag über Viren gehalten - welchen Schaden sie anrichten etc... .
Abschließend hat er dann ein paar ganz besonders lustige Viren am PC vorgeführt. Einer davon spielte z.B. alle 10 Minuten im kontaminierten Programm die US-Nationalhymne. Darauf eine unserer Sekretärinnen: 'Das kann kein Virus sein, das macht meine Textverarbeitung auch immer!'
Darauf wurden die Herren der oberen Etage irgendwie kreidebleich...
From: Michael Simons, simons@i6.informatik.rwth-aachen.de

Viren kosten den Computeranwender Geld. Entweder für Anti-Virenprodukte, für die Virenbeseitigung und für Schäden, die ein nicht rechtzeitig entdeckter Virus anrichten kann. /vgl. hierzu Lan, S. 45, er nennt auch Zahlen, die jedoch aus dem Jahre 1993 sind und auf Schätzungen beruhen/ Selbstverständlich können Anti-Virenprodukte keinen vollständigen Schutz bieten, aber sie entdecken und beseitigen doch einen Großteil der Viren. Sie sind mittlerweile in guten Programmpaketen enthalten. Aber der Computeranwender muss sie halt auch anwenden. Insbesondere nach einem Besuch im Internet empfiehlt es sich, einen Virenscanner durchlaufen zu lassen. Dies benötigt ca. zwei Minuten Aufwand und die sollte man für einen (durch diese Vorsichtsmaßnahme doch wahrscheinlich) virenfreien Rechner opfern.

5.1 Struktur eines Computervirus

Ein Computervirus ist prinzipiell immer gleich strukturiert. Die Definition und die Strukturbeschreibung eines Computervirus wird von Langemeyer direkt übernommen, denn er hat dieses auch für den Laien verständlich in einfachen Worten erklärt. Ausführlicher sind Stang /ICS/ und Slade /Sla/. Ihre Beschreibungen der Struktur und auch der Vorgehensweise der Viren sind interessant (und wichtig), wenn man tiefer in die Materie eindringen will. Nur zur Definition von Langemeyer soll angemerkt werden, dass die Vermehrung nicht nur unkontrolliert, sondern auch in fast allen Fällen lange Zeit unbemerkt stattfindet.

“Definition:

Ein Computervirus ist ein Stück Programmcode, das sich aus einem Programm heraus vom Benutzer unkontrolliert vermehrt, in dem es Kopien von sich an andere Programme anhängt.

Damit unterscheidet sich der Computervirus vom Computerwurm, der ein selbständiges Programm darstellt und somit kein Wirts-Programm benötigt.

Die Bezeichnung `Virus´ ist aus der Medizin entlehnt, da einige Parallelen festzustellen sind. Die Übertragung von Virenbekämpfungsmethoden der Medizin auf den Computervirus hat die Entwicklung von Antivirenprogrammen erleichtert.

> Ich bin Hiwi hier an der Uni Mannheim und erteile für andere Studis auch EDV-Kurse. Letztes Semester, während eine Anfänger-Veranstaltung, erzählte ich von Viren und Virenscanner, um den Neulingen einen kleinen Überblick zu geben.
> Kurz danach, während eine Pause, fragte mich ein Student (mit einem ziemlich besorgten Gesichtausdruck): "Sag mal, wenn so ein Computer Viren hat und ich davor sitze, kann mir auch was passieren?"
> Ich konnte mich nicht zurückhalten und sagte: "In diesem Pool sind schon 3 Leuten daran gestorben, ich hab es gesehen!"
> From: Patrizia Prudenzi, patricia@umav32.verwaltung.uni-mannheim.de

Der Virus ist meistens an ein Computerprogramm angehängt (Link-Virus) oder überschreibt Teile des Programms, insbesondere bei größeren Programmen. Der Virus besteht aus folgenden Teilen:

⇒Transportteil

Dieser Teil kopiert den Virus in den Arbeitspeicher des Rechners und verkettet ihn mit dem Betriebssystem. Von dort aus überwacht der Virus z.B. den Wechsel von Disketten, um diese zu infizieren. Aus dem Betriebssystem heraus ist insbesondere der Tarnkappenvirus in der Lage, durch geeignete Maßnahmen die Suche nach ihm zu erschweren. Der Transportteil ist jedoch nicht in allen Viren zu finden.

⇒Vermehrungsteil

Der Vermehrungsteil sucht auf den Datenträgern nach noch nicht infizierten Programmen. Dazu benutzt er teilweise Kennungen wie ein biologischer Virus. Eine solche Kennung ist zum Beispiel die Sekundenangabe: 62 Sekunden in dem Dateiverzeichnis des Datenträgers (Eine Sekundenangabe > 59 ist per Definition nicht möglich). Er versucht, ein Programm zu infizieren: Eine Kopie des Virus wird an das Programm angehängt oder in das Programm hineingeschrieben. Die Startadresse auf den Anfang des Virus gesetzt und die Startadresse des Programms an den Virus angehängt. Dadurch werden beim Start des infizierten Programms erst der Virus und dann das Programm ausgeführt.

⇒Wirkteil

Das eigentliche Ziel des Computervirus ist es, irgendeinen Schaden im Rechner zu bewirken. Dies kann eine harmlose Meldung auf dem Bildschirm sein, kann im Löschen der Festplatte bestehen oder gar im sporadischen Verändern von Dateien ausarten. Diese sind besonders schwer festzustellen und praktisch nicht mehr zu korrigieren.

Damit ein Virus nicht vorzeitig auffällt und genügend Zeit zur Vermehrung bleibt, erfolgt die Wirkung ereignisgesteuert. Beispiele für solche Ereignisse sind: Freitag, der 13.; der 6. 3., Geburtstag von Michelangelo, eine gewisse Anzahl von Infektionen.” /Lan, S.47 und 48/

To: ORAKEL
Subj: Antivirenprogramme

Liebes Orakel,
bietet das Rechenzentrum (oder sonst wer an der Uni) aktuelle Virenprogramme (MS-DOS) an? Mein Chef hat mehr Angst vor Computerviren als vor AIDS.

MfG XXXXXXX Angewandte Physiologie
From: RZMAIN::XXXXXX

5.2 *Strategie gegen Viren*

Am besten ist natürlich, man hat keine Viren auf dem Rechner und man gibt den Viren auch keine Chance auf den Rechner zu gelangen. Das ist jedoch nur bei Rechnern möglich, die (sozusagen) keinen Kontakt nach außen haben. Z.B. Stand-Alone PCs, die keine Diskette sehen, die auf einem anderen Rechner benutzt wurden und auch sonst über keine Datenübertragungsmöglichkeit verfügen.

Der gewöhnliche Rechner bekommt jedoch Daten, Dateien und/oder Programme per Diskette eingespielt oder anderweitig übertragen. Oft sind die Rechner an irgend ein Netz angeschlossen, wodurch sich die Infektionsgefahr erhöht. Das Internet gilt als einer der größten Infektionsübertrager, obwohl auch hier einiges getan wurde, um die Gefährdung durch Viren zu mindern. Aber Warnungen sind sinnlos, wenn sie nicht beachtet werden, die beste Anti-Viren-Software ist nutzlos, wenn sie nicht angewendet wird.

Langemeyer beschreibt nun allgemein, wie man Virenbefall vermeiden kann; falls er doch passiert ist, wie man ihn erkennen kann und die Viren beseitigen kann. Der Leser, dem die von Langemeyer übernommenen Beschreibungen und Vorschläge nicht detailliert genug sind, sei auf folgende Literatur verwiesen:

⇒ ICSA´s Computer Virus Handbook von David J. Stang /ICS/
⇒ Robert Slade`s Guide to Computer-Viruses /Sla/
⇒ oder falls man über einen Internetanschluß verfügt: Nick FitzGerald, frequently asked questions on Virus-L/comp.Virus /Fit/

Ich versuche vor ca. 10 Leutchen, jeder vor einem Terminal sitzend, einen login in den Großrechner zu erklären:
Ich: "Tippen sie bitte dort wo der Cursor blinkt (Unterste Zeile) 'login' ein und danach die Datenfreigabetaste betätigen."
DAU: kurz danach: "uuuuuuhhhhhhhhooaaahhhhh ..."
Ich: (In Gedanken:) "Was macht der denn da??" und marschier zum DAU hin.
DAU: Immer noch gebannt auf Monitor schauend
Ich: Erkenne, dass DAU mit zunehmender Begeisterung der Tastenwiederholung zusieht
Übrigens, der Aufschrei von ihm war dadurch begründet, dass das 'n' von loginnnnnnnnnnn... nach erreichen des Zeilenendes ganz oben in der ersten Zeile wieder aufgetaucht ist.
Nachdem der Bildschirm voller 'n's war, sagte ich zum DAU:
"Na wenn das nicht ein VIRUS war ..."
DAU: erschrocken mich anblickend "EIN VIRUS??"
Ich: "Möglich iss alles."
DAU: Zieht seine Hände von der Tastatur weg und schaut seine Finger ganz entsetzt an
Und da soll einer gefasst und ohne eine Miene zu verziehen danebenstehen ...

From js@barbar.abg.sub.org

5.2.1 Virenbefall verhindern

Virenbefall verhindert man durch Computerhygiene. Dazu hat Langemeyer vier Vorschläge, von denen der wohl wirkungsvollste Vorschlag die Softwarehersteller betrifft. Die anderen Vorschläge betreffen den Anwender; Vorschlag 2 setzt aber voraus, dass der Anwender über Antivirensoftware verfügt:

⇒Die Datenträger für Programme sind mit absolutem Schreibschutz zu versehen. Das BSI empfiehlt sogar den Herstellern Disketten ohne Schreibschutzschieber zu versenden.

⇒“Fremde (auch gekaufte) Programme sind vor dem ersten Einsatz unbedingt auf Viren zu untersuchen.

⇒Rechner dürfen nicht unbeaufsichtigt Fremden zugänglich sein (möglichst den Diskettenschacht verschließen).

⇒Daten sind rechtzeitig und regelmäßig zu sichern.” /Lan, S. 48,49/

⇒Der fünfte Vorschlag klingt wie Werbung der Softwarehersteller - aber mit der beste Virenschutz ist die Verwendung korrekt beschaffter Software in den Original-Disketten, die schreibgeschützt sind oder CDs.

5.2.2 Virenbefall feststellen

Um Viren festzustellen, kann man Anti-Viren-Software benutzen aber es gibt auch Kennzeichen am Rechner, die ohne spezielle Software feststellen lassen, ob ein Verdacht auf Virenbefall besteht. Ausführlich werden die einzelnen Antivirensoftware-Produkte und ihre Wirkungsweise bei Slade /Sla, S. 145 ff. und dessen Anhänge C,D,E/ beschrieben. Dies ist hier jedoch zu weitgehend, es genügen die von Langemeyer beschriebenen Fakten:

⇒“Suche nach bekannten Viren

Mit Hilfe von Virensuchprogrammen, oft auch Virenscanner genannt, wird jedes neue Programm auf die Viren untersucht, die der Virenscanner kennt. Aufgrund des Anwachsens der Virenzahl ist es sinnvoll, für ein solches Programm ein Update zu abonnieren. Um möglichst viele Viren zu erfassen, sollte die letzte Version nicht älter als ein Vierteljahr sein. Aber der Einsatz auch älterer Programme vermindert zumindest das Infektionsrisiko.

⇒Überwachung von Virenaktivitäten

von einem im Hintergrund arbeitenden Überwachungsprogramm werden typische Virenaktionen vermerkt, werden kritische Kombinationen solcher Aktivitäten erkannt, wird ein Alarm ausgelöst.

⇒Prüfung auf Programmveränderung

Zum Auffinden der von Virensuchprogrammen bisher unentdeckten Viren dienen Signaturprogramme. Sie ermitteln von neu eingesetzten Programmen Kontrollwerte. Diese Werte werden möglichst täglich neu ermittelt und gegen

die alten verglichen. Bei Differenzen wird eine entsprechende Warnung ausgegeben.” /Lan, S.49/

Es ist sehr wichtig, dass diese Programme, d.h. Virenscanner und Signaturprogramme sicherstellen, dass sie selbst nicht verändert werden. Ebenso soll das Betriebssystem durch diese Programme vor (ungewünschten) Veränderungen bewahrt werden.

Die Vorschläge Langemeyers setzen voraus, dass man über Antiviren-Software verfügt. Manfred Drechsel /Dre/ gibt einige Hinweise, wie man auch als `Laie´ feststellen kann, ob ein Verdacht auf Virenbefall besteht, wenn man über keine Antiviren-Software verfügt. Selbstverständlich hat man schon Viren auf dem Rechner, wenn die folgenden Beobachtungen zutreffen:

⇒“Programme brauchen für den Start länger als üblich.

⇒Programme versuchen ohne Grund, auf Diskettenlaufwerk oder Festplatte zuzugreifen.

⇒Der verfügbare Festplattenplatz oder Hauptspeicher verringert sich auf unerklärliche Weise.

⇒Die Last auf dem Netzwerk ist unerklärbar hoch.” /Dre/

Ähnliche Tipps geben auch Stang und Slade; weitere, noch für den `Laien´ erkennbare Anzeichen sind:

⇒Die Größe der Programme ändert sich.

⇒Das Datum der letzten Änderung hat sich geändert.

⇒Die `Directory´-Struktur hat sich geändert.

⇒Die Adressen (Monitor, Tastatur, bei Netzanschluss die Serveradresse usw.) haben sich geändert.

⇒Programme sind verschwunden.

⇒Unverlangte Neustarts

Viren-Erkenntnisse nach Murphy:
Computerviren verbreiten sich prinzipiell über garantiert unverseuchte Programm- und Betriebssystemdisketten. Du bekommst einen Computervirus genau dann, wenn du ihn am wenigsten brauchen kannst. Garantiert ungefährliche und leicht zu entfernende Viren bekommen immer nur die anderen. Du hast immer einen Virus mehr, als du glaubst. Wenn du von all deinen Dateien ein Backup hast, hat der Virus auch diese bereits verseucht. Ein Virensuchprogramm, auf deinem Computer eingesetzt, wird bei seinem Suchlauf alle Text- und Programm-Dateien irreparabel zerstören und lediglich den Virus übriglassen. Folgerung: Das einzige, was am Ende auf deinem Computer noch lauffähig ist, wird der Virus sein.

von Holger Weisser
email:weisser@rz1a.rz.fh-wilhelmshaven.de

Wenn es schon soweit ist, dass sich die Arbeitsprogramme nicht mehr starten lassen oder dass die Buchstaben des auf Bildschirm angezeigten Textes runterfallen, ist es für Vorsorge wirklich zu spät und man muss die Virenbeseitigung in Angriff nehmen. Den dafür notwendigen Aufwand kann man relativ klein halten, wenn man auf die Virenbeseitigung vorbereitet ist.

5.2.3 Vorbereitung zur Virenbeseitigung

Die Hauptarbeit bei der Vorbereitung zur Virenbeseitigung ist das Zusammenstellen der für die Neuinstallation des Rechners notwendigen Unterlagen. Diese Unterlagen sollten auf dem neusten Stand gehalten werden. Dazu zählen neben den Disketten und CDs auch die dazu notwendigen schriftlichen Unterlagen (z.B. Installationsanleitungen und Programmbeschreibungen). Man spricht hier auch vom `Status Quo Paket´. Dies enthält insbesondere:

⇒einen aktuellen "Ausdruck der Systemdateien z.B. CONFIG.SYS und AUTOEXEC.BAT

⇒Listen der Directory-Struktur, der Partitionen auf der Festplatte (Graphischer Baum)

⇒Übersicht der verwendeten Software-Produkte

⇒Partitition-Table und CMOS-Setup

⇒`DISKMAP´ der Festplatte / Partition

⇒Für die im Rechner zusätzlich eingebauten Platinen die eingestellten Adressen, Interrupts und Jumper-Settings

⇒Sämtliche Handbücher der Anwendungen

⇒Aktuelle PC-Checkliste für das Gerät

⇒Name und Telefonnummer. von:

- ◊ Organisator / Betreuer in der Abteilung
- ◊ Zuständiger Sicherheitsbeauftragter

⇒Aufstellung der Abteilungen / PC mit denen Daten und/oder Programme ausgetauscht werden.

⇒MS-DOS-Systemdiskette (natürlich bootfähig und virenfrei)

⇒Erforderliche Treiberprogramme

⇒Oberflächen bzw. Menüsysteme

⇒Konfigurationsdateien von Anwendungen (z.B. WIN.INI von MS-Windows)

⇒Programm-Diskette der verwendeten Sicherungs-Software (Fastback, Turbo-Backup, Streamer-Software, etc.)

⇒Sämtliche Original-Disketten der Anwendungen

⇒Mindestens die letzten zwei Datensicherungen" /Lan, S.50/

Der letzte Punkt dieser Liste ist ein neuer Gefahrenherd. Die zwei letzten Datensicherungen sind vorher durch einen Virenscanner zu prüfen, ob sie nicht doch infiziert sind, bevor sie in den Rechner überspielt werden.

5.2.4 Virenbeseitigung

Wenn man nun erkannt hat, dass der Rechner einen Virenbefall hat, gibt es zwei Möglichkeiten, die Viren zu entfernen. Die erste Möglichkeit setzt jedoch voraus, dass man über einen entsprechenden Virenscanner besitzt. Die meisten Virenscanner enthalten auch Hilfen, um Viren zu beseitigen. Dies ist eine bequeme, schnelle und in vielen Fällen erfolgreiche Methode, diese Hilfen auch zu benutzen. Viele Viren werden so auch erwischt und entfernt./Sla/ Trotzdem rät Langemeyer /Lan/ von der Benutzung eines Virenscanner-Hilfsprogramms ab. Er bezeichnet dies sogar als gefährlich. Es besteht schließlich die Gefahr, dass der Virenscanner den Virus nicht sauber erkannt hat. Bei dem entdeckten Virus kann es sich um eine Abart des vermuteten Virus handeln, der aber einen veränderten Aufbau hat. Die Folge kann nun sein, dass bei der Virenbeseitigung zuviel oder zuwenig aus dem befallenen Programm herausgeschnitten wird. Im ersten Fall kann es sein, dass das betroffene Programm fehlerhaft oder gar nicht mehr funktioniert. Im zweiten Fall kann es sein, dass sich der Virus von neuem entwickelt und im Rechner verbreitet. Slade /Sla/ rät von dieser Methode nicht ab, erwähnt jedoch, dass man Schwierigkeiten haben kann, das Antivirenprogramm zu starten oder dass es selbst befallen werden kann. /Sla, S. 30/
Langemeyer empfiehlt daher nur die zweite Möglichkeit - die Neuinstallation. Dies bedeutet also, dass die ganzen Massenspeicher des Rechners gelöscht werden und alle Programme und Dateien - auch das Betriebssystem - neu geladen werden. Verfügt man über ein Status-quo-Paket, benötigt man für die Neuinstallation relativ wenig Zeit. Er empfiehlt noch, die verseuchten Dateien/Programme auf extra, deutlich gekennzeichnete Disketten zu kopieren. Damit hat man dann die Möglichkeit, den Virus eindeutig zu identifizieren. Bewährt hat sich nach seinen Worten die BERT-Methode:

⇒“**B**ooten des Systems von einer virenfreien Systemdiskette

⇒**E**ntfernen der infizierten Dateien durch Überschreiben

⇒**R**estaurieren durch Einspielen der Originaldateien

⇒**T**esten des Systems mit aktuellen Virensuch- und Signaturprogrammen.” /Lan, S. 51/

Wichtig ist - wie in allen Schadensfällen - die Nerven bewahren und nicht hektisch werden. Sonst zerstört man vor lauter Nervosität mehr als man repariert. Man sollte sich mit dem System auskennen, andernfalls muss man halt

Hilfe besorgen. Wenn wichtige - gar unter das Bundesdatenschutzgesetz fallende - Daten betroffen sind, sollte man den Vorgesetzten und den Sicherheitsverantwortlichen informieren.

Diesseits von Ebola

Grippewellen, Allergien und Computerviren überfluten unser Land. Besonders letztere werden immer gefährlicher. Die Nachfolger des berüchtigten Michelangelo-Virus sind inzwischen völlig unabhängig von der verwendeten Hardware. Sie breiten sich auf Rechnern aller Art aus, sowohl in Politik und Wirtschaft als auch im Showbusiness.

Sogar Parlamente und Parteiapparate sind nicht mehr sicher vor ihnen. Parlamentarische Immunität, eine typische Softwarelösung der vergangenen Jahre, bietet mittlerweile keinerlei Schutz mehr. Computersysteme, Datennetze und Institutionen reagieren zunehmend allergisch auf die neue Generation von Viren.

Hier einige der gefährlichsten Exemplare:

Rexrodt-Virus:

Das gesamte System wird nach und nach lahmgelegt, aber der Bildschirm meldet unbeirrt drei Prozent Wachstum.

Kanther-Virus:

eines der wenigen Viren-Programme, das ausschließlich in deutscher Sprache geschrieben wurde. Schiebt sämtliche fremdsprachigen Programme und Dateien ohne Rücksicht auf Datenverluste ins elektronische Niemandsland ab. Bis die Festplatte komplett deutsch ist und einen ordentlichen Scheitel hat.

Schmidtbauer-Virus:

durchforstet Festplatten und andere Peripheriegeräte nach Plutonium. Wird das Virus fündig, meldet es optisch und akustisch: Gefahr aus dem Osten! Anschließend zerstört es sämtliche Daten, so dass nichts bewiesen werden kann.

von Wolfgang Mocker, im Eulenspiegel 7/95 (gekürzt)

6 Beschaffung oder Erstellung und Einführung eines Programms für Arbeitsschutz

Als Fachkraft für Arbeitssicherheit (FaSi) ist man nach gesetzlichem Auftrag für viele Dinge zuständig. Man soll sich um die sicherheitsgerechte Ausgestaltung des Maschinenparks kümmern (Maschinen im weitesten Sinne - so zählen auch Computerarbeitsplätze dazu wie den Ausführungen in Kpt. 3 zu entnehmen war), den Schutz der Arbeitnehmer vor Gefahrstoffen, Strahlung, Brandgefahren usw. organisieren und ist oft auch noch über den gesetzlichen Auftrag hinaus für Umweltschutzbelange und Abfallwirtschaft zuständig. Um all diese Aufgaben effektiv erledigen zu können, sollte man über gute Hilfsmittel verfügen. Ein solches Hilfsmittel kann eines der Programme sein, die insbesondere in neuerer Zeit für das Aufgabenfeld Arbeits- und Umweltschutz entwickelt worden sind. Diese Programme sind immer besser und auch preisgünstiger geworden. Trotzdem liegen die Kosten für eine umfangreiche Lösung immer noch in einer Größenordnung, die es nahe legt, solch eine Investition auch unter betriebswirtschaftlichen Aspekten zu tätigen und organisationstechnische Methoden bei der Beschaffung oder Erstellung einer entsprechenden Lösung zu benutzen.
In der Organisationstechnik haben sich in der praktischen Anwendung Phasenkonzepte als brauchbares Hilfsmittel zur Strukturierung der Vorgehensweise bei der Planung und Realisation einer EDV-Einführung oder Änderung bewährt. /vgl. Utt, S. 20/ Solch ein der Organisationstechnik entlehntes Phasenkonzept zur Einführung oder Änderung von EDV für den Arbeitsschutz empfehlen auch Hartung /Har2, S. 27 ff./ und der Arbeitskreis `EDV im Arbeitsschutz´ des VDSI./Sas, S. 26 ff./
Das Ziel eines solchen Phasenkonzepts ist die Zerlegung der Planung und Durchführung eines EDV-Vorhabens in überschaubare Arbeitsschritte (Phasen, Stufen). Dies ermöglicht eine eigenständige Bearbeitung einzelner Phasen, so dass in jedem Stadium der Arbeit (notfalls) auch ein unterschiedlicher Personenkreis involviert sein kann.
"Ziel der Vorgehensweise ist es, zunächst eine vorhandene Problemstellung zu analysieren und Lösungen für deren Durchführung zu entwickeln und zu bewerten. Eine immer weitergehendere Gliederung in Teilprobleme bzw. Teillösungen führt dazu, dass im letzten Stadium komplexe Zusammenhänge für die einzelne Teillösung in einfache Beziehungen aufgelöst sind, die für sich genommen leicht realisierbar (im Sinne von programmierbar oder einführbar) sind.
Jede Phase soll nach ihrem Abschluss ein Ergebnis liefern, das es ermöglicht, über die weitere Fortführung des Projektes zu entscheiden.

Es ist direkt einsichtig, dass je früher in diesem Prozess eine Zielrichtung korrigiert werden kann, sich die finanziellen Aufwendungen begrenzen lassen. Zugleich dient die Zerlegung in Phasen dazu, den Fortgang der Entwicklung zu dokumentieren und eine Kontrolle über den zeitlichen Ablauf zu erhalten (Projektverfolgung)." /Utt, S. 20/

Utter verwendet das Phasenkonzept von Becker /Bec, S. 199/ kombiniert mit den ADV-Projektrichtlinien des Bundes und der Länder /Gru, S. 23/ für ein eigenes Phasenkonzept /Utt, S. 28/, das hier durch das Phasenkonzept von Hoffmann /Hof, S. 132/ ergänzt und an die Belange des Arbeitsschutzes angepasst ist und in Tabelle 6-1 dargestellt ist.

Man wird in der Praxis - als FaSi - sich wohl kaum die Zeit nehmen können, alle Punkte dieser Konzepte, z.B. anhand des Phasendiagramms nach Gerken (wie es im Anhang 6-1 als Tabelle 6-2 dargestellt ist) abzuarbeiten. In dieser Tabelle 6-2 sind insbesondere die Punkte Voruntersuchung, Systemanalyse und Systementwurf in viele wichtige Unterpunkte aufgeschlüsselt. Man spürt bei diesem Konzept von Gerken ganz deutlich, aber auch bei anderen organisationstechnischen Konzepten, dass sie eigentlich für größere EDV-Planungen gedacht sind als es die Beschaffung eines Programms für Arbeitssicherheit mittlerweile darstellt. Trotzdem sollte man sich im wesentlichen nach diesen Konzepten richten, um unliebsame Überraschungen bei Beschaffung und Verwendung der Programme zu vermeiden.

Wenn man den Textumfang sieht, könnte man glauben, dass die Überlegungsfase die wichtigste und zeitaufwendigste Fase ist. Die wichtigste Fase wird es sein, denn hier werden die Grundentscheidungen getroffen. Je nach der Vorarbeit, die in dieser Fase geleistet wird, können die nächsten Fasen einerseits weniger zeitaufwendig sein als diese Fase. Andererseits werden jedoch insbesondere bei Eigenprogrammierung die Phasen „Systementwurf“ und „Systemerstellung“ deutlich zeitintensiver sein.

Phasen-nr.	Phase	Aufgaben
0	Vorphase: Überlegensfase	Prinzipielle Klärung der Frage, ob die Einführung oder Änderung der EDV für Arbeitsschutz notwendig ist.
1	Systemanalyse	Das Aufgabenfeld der FaSi wird funktions-orientiert bestimmt (Systemabgrenzung) und die einzelnen Elemente der Tätigkeit analysiert (Systemerhebung) und schriftlich fixiert (Systembeschreibung/-dokumentation).
2	Zielfestlegung	Kritische Überprüfung der Ergebnisse der Systemanalyse; Bestimmung der Hauptziele des einzuführenden oder anzupassenden EDV-Systems für Arbeitsschutz.
3	Durchführbarkeitsstudie	Wirtschaftliche, technische, informatorische Einschränkungen werden erfasst und die festgelegten Hauptziele auf ihre Durchführbarkeit unter diesen Bedienungen überprüft.
4	Sollkonzeption	Die Aufgabendefinition des EDV-Systems und der dafür notwendige Grundaufbau des Systems wird in einem Pflichtenheft zusammen gefasst.
5	Systementwurf oder Systembeschaffung	Bei einer Neu- oder Umprogrammierung erfolgt die detaillierte Beschreibung. Anderenfalls erfolgt die Beschaffung anhand den im Pflichtenheft festgelegten Kriterien.
6	Systemimplementierung	Soweit noch nicht geschehen, räumliche, organisatorische und personelle Voraussetzungen schaffen. EDV-System einführen, bzw. umstellen. Fehler erkennen und beseitigen; System bewerten und abnehmen.
7	Systembetrieb	Routinemäßige Arbeitsphase mit Systempflege.

Tabelle 6-1 Phasenkonzept zur Einführung oder Anpassung eines EDV-Systems für Arbeitsschutz /in Anlehnung an Hof, S.132/

6.1 Überlegensphase/Voruntersuchung

Es kann von drei verschiedenen Vorraussetzungen ausgegangen werden:

- Man steht in der Überlegungsphase, ob EDV in der Arbeitsschutzabteilung eingeführt werden soll.
- Es besteht die Prämisse, dass EDV eingeführt werden soll.
- EDV ist vorhanden, die vorhandene Software soll ergänzt/aktualisiert werden.

Insbesondere, wenn man in der Überlegungsphase ist, ob überhaupt EDV in der Arbeitschutzabteilung eingeführt werden soll, sollte man sich mit den folgenden Fragen beschäftigen:

1. Bietet ein EDV-Einsatz im allgemeinen Vorteile?

Hier muss man ganz generell bewerten, ob sich die Kosten für die Beschaffung eines Computers und entsprechender Software im Verhältnis zu einer vielleicht möglichen Arbeitsersparnis rechnen. Mögliche Arbeitsersparnisse können sein:

- Bequemere und oft auch schnellere Textbearbeitung;
- schon ausgefüllte Formulare können wiederverwendet werden;
- automatisches Erstellen von Tabellen u.ä.;
- automatische Auswertung von Tabellen/Dateien;
- besserer Informationszugriff;
- Wiederverwendbarkeit von bereits erstellten und nur wenig zu ändernden Unterlagen usw.

2. Wenn ja, welche dieser Vorteile sind für die Arbeitsschutzabteilung bzw. FaSi von Interesse?

Es ist einsichtig, dass alle obengenannten Punkte auch für eine Arbeitsschutzabteilung bzw. eine FaSi von Interesse sind. Hier bleibt dann nur noch die Frage offen, ob die vorhandene Arbeitsmenge, die diese Vorteile ausnützt, den notwendigen Kapitaleinsatz rechtfertigt. Dazu muss parallel festgestellt werden (falls das noch nirgends fixiert wurde) oder es muss schon bekannt sein (d.h. fixiert sein), welche Aufgaben die Abteilung/die Fachkraft für Arbeitssicherheit in der Regel zu bearbeiten haben. In Tabelle 6-3 (als Anhang 6-2) werden die Aufgaben einer FaSi aufgezählt, wie sie von Grassl/Sinks festgestellt wurden. Die wesentlichen Aufgaben sind kurzgefasst in der Regel (oft hat eine FaSi über den gesetzlichen Auftrag hinausgehende Aufgaben) folgende:

- Arbeitsbereichsanalysen
- Arbeitsplatz-, Anlagen-, Maschinenüberwachung
- Erstellen von Sicherheitsvorschriften
- Ausbildung, Schulung, Unterweisung

- Verwaltung der persönlichen Schutzausrüstung
- Unfalldatenbearbeitung (Erfassung, Verarbeitung, Auswertung)
- Gefahrstoffverwaltung
- Erstellen von Betriebsanweisungen
- Erstellen von Sicherheitsdatenblätter
- Erstellen von Unfallmerkblättern
- Gefahrgut
- Abfallentsorgung/-management
- Immissions-, Emissions-, Gewässerschutz
- Kontakt, Zusammenarbeit mit Betriebsleitung, Betriebsrat, Behörden

Die nächste Frage ist

3. Welche Aufgaben einer Fachkraft für Arbeitssicherheit sind geeignet zur rationellen Bearbeitung mittels EDV-Einsatz?

Sie kann nun mit der Kenntnis der Aufgaben der FaSi beantwortet werden:

- Der allgemeine Schriftverkehr kann mit dem Hilfsmittel Textverarbeitung durchgeführt werden. Auch der fachspezifische Schriftverkehr, der bei der sicherheitstechnischen Beratung von Vorgesetzten, Unternehmern, Behördenleitern etc. anfällt, kann ebenfalls mit einem 'normalen' Textverarbeitungssystem durchgeführt werden.
- Die Aufnahme, Bearbeitung, Verwaltung und Auswertung von Arbeitsstoffen (Gefahrstoffe und andere chemische Stoffe) bietet großen Raum für eine EDV-Unterstützung. Hier kann an sich mit einer `marktüblichen´ Datenbank gearbeitet werden. Aber der Zeitaufwand für die Anpassung solch einer Datenbank (entsprechende Masken erstellt, Gefahrstoffdaten eingegeben) bis diese Datenbank im gewünschten Sinne lauffähig ist, ist für eine FaSi sehr groß, insbesondere falls diese nicht mehr als Computergrundkenntnisse besitzt. Auf dem (deutschen) Markt werden recht viele (Software-) Lösungen angeboten, die das Thema Gefahrstoffe vollständig abdecken. Es wird wohl für einen Betrieb (eine FaSi) rentabler sein, die sofort nutzbare, wenn auch teurere Spezialsoftware zu kaufen als eine gewöhnliche Datenbank anzupassen. Eine weitere Möglichkeit wäre die Beschaffung von vorbereiteten Tools, welche auf eine `marktübliche´ Datenbank aufsetzbar sind und die Programmierarbeit wesentlich erleichtern und beschleunigen.

- Auch bei der Gestaltung und Bewertung von Arbeits- und Produktionsverfahren unter Berücksichtigung der Punkte: sichere und gleichzeitig rationelle Arbeitsabläufe, sicherheitsgerechte und wirkungsvolle Arbeitsmittel, gefahrenfreie und praktische Gestaltung und Aufbau der Arbeitsplätze oder Arbeitsbereiche sowie einer gesunden und ergonomischen Arbeitsumgebung bieten sich Datenbanken als Hilfsmittel an. Auch hierfür gibt es Software, die den Anforderungen einer FaSi entsprechen. Entsprechende Checklisten und deren Auswertung durch das Programm erleichtern die Arbeit einer FaSi deutlich. Hier könnten vorbereitete Tools, die auf eine marktübliche Datenbank aufgesetzt werden, eine preisgünstige Alternative sein.
- Die Erstellung von Arbeitsanweisungen, Richtlinien und Merkblättern (z.B. für den Umgang mit Gefahrstoffen) kann mit Hilfe einer Datenbank sowie eines Textverarbeitungsprogramms deutlich erleichtert werden. Hierfür werden spezielle fertige Lösungen angeboten, die in der Regel auf Gefahrstoffdatenbanken zugreifen. Häufig sind diese Aufgabenteile auch bereits in den Gefahrstoffdatenbanken enthalten.
- Die Einführung, Änderung und Verwaltung der Persönlichen Schutzausrüstung kann gleichfalls mittels einer gewöhnlichen Datenbank und einer Textverarbeitung vereinfacht werden. Hierfür wie auch für den nächsten Unterpunkt werden fertige Lösungen angeboten, die oft Teil eines Gesamtpaketes zur rechnergestützten Arbeitserleichterung einer FaSi sind.
- Für die Überprüfung von Grundstücken, Gebäuden, anderen baulichen Anlagen sowie technischer Anlagen kann ein sogenannter elektronischer Kalender und eine z.B. in einem Textverarbeitungsprogramm erfasste und gespeicherte Checkliste eine Hilfe sein.
- Ein Textverarbeitungsprogramm ist auch sinnvoll als Hilfsmittel beim Mitteilen der beim Beobachten festgestellten Mängel. Das Vorschlagen von Maßnahmen zur Beseitigung der festgestellten Mängel kann ebenfalls mittels eines innerhalb einer Textverarbeitung gespeicherten Formblattes effizienter gestaltet werden.
- Weitere Aufgaben wie Schulung und Betreuung der Sicherheitsbeauftragten, die Zusammenarbeit mit dem Betriebs-/Personalrat, dem Betriebsarzt, außerbetrieblichen Stellen des Arbeitsschutzes usw. können ebenso durch den Einsatz einer Textverarbeitung bezüglich des Schriftverkehrs unterstützt werden.
- Je nach anfallender Menge der Schadensmeldungen, der Beinahe-Unfälle und der Unfälle wird bei der Aufnahme und Speicherung der hierbei anfallenden Daten eine Datenbank von Nutzen sein. Für die Auswertung dieser Daten kann ein Statistikprogramm eine wesentliche Unterstützung darstellen. Der notwendige Schriftverkehr wegen dieser Ereignisse mit z.B. der Geschäfts-/

Behördenleitung sowie dem Unfallversicherungsträger (bei Anfallen von meldepflichtigen Arbeitsunfällen) kann mit Hilfe einer Textverarbeitung ebenso rationalisiert werden.

Die eigentlichen Kontroll- bzw. Überwachungsaufgaben können derzeit (2000) nur unter sehr großem finanziellen und technischen Aufwand mittels Computersysteme vereinfacht oder gar automatisiert durchgeführt werden.

Nach dieser Überlegung und Zusammenstellung von Aufgaben können die letzten zwei Fragen in der Überlegensphase beantwortet werden:

4. Sind dies genügend Aufgaben, die einen Kapitaleinsatz zum Kauf eines Rechners, der Programmierung mit Hilfe von Tools oder zum Kauf immer noch relativ kostenintensiver Spezialprogramme rechtfertigen?
5. Geben andere, z.B. externe Anlässe den Grund für die Einführung von EDV?

In der Diskussion dieser Fragen/Überlegungen zu diesen Fragen werden zweifellos folgende Punkte angeschnitten/berücksichtigt werden:

- Die Neubildung oder Umstrukturierung einer Arbeitsschutzabteilung erfordert ohnehin eine Umgestaltung der bisherigen Arbeits- und Informationsmethoden.
- Das aufzunehmende und zu bearbeitende Daten- und Informationsvolumen ist derart expandiert (z.B. durch die Aufgabe der Gefahrstofferfassung), dass neue Verarbeitungsmöglichkeiten ins Auge gefasst werden müssen.
- Bisherige Methoden zur Daten- und Informationsbereitstellung erfüllen nicht mehr die geforderten Belange, da sich interne (u.a.. steigende Zahl von Mitarbeitern, veränderte Stoffe und Produktionsmethoden) und externe Bedingungen (möglicherweise neue Vorschriften, neue Lieferanten) geändert haben.
- Die Ansprüche an den Bedienungskomfort. zur Informationsbereitstellung können gestiegen sein. Es genügt in vielen Fällen nicht mehr auf Stofflisten nach alphabetischer Ordnung zuzugreifen, sondern es müssen noch andere Sortierkriterien möglich sein wie Gefahrenklasse, typische Eigenschaften etc.
- Selbstverständlich spielen auch direkte Kostenüberlegungen eine wichtige Rolle; da Personalkosten einen sehr hohen Anteil an den Gesamtkosten einer Arbeitsschutzabteilung haben, wird versucht werden, zumindest zusätzliches Personal zu vermeiden, um obige Probleme zu lösen.

Die bisher genannten Punkte haben einen ökonomischen Hintergrund. Bei der Entscheidungsfindung können auch folgende nichtökonomische Punkte eine ganz bedeutsame Rolle spielen:

- Um einen bestehenden Ruf nicht zu verlieren (Firmenimage), kann es notwendig sein, auch Arbeiten, die nicht unbedingt EDV-Einsatz erfordern, mittels EDV durchzuführen.
- Um die Modernität der Firma zu wahren, ist nach allgemeiner Auffassung ein EDV-Einsatz - auch im Arbeitsschutz - unvermeidbar.
- Eine in dieser Richtung ausgeprägte Firmenphilosophie ist weiterer Anlass; auch hier geht es um den Ruf der Firma.

Hinzu können noch externe Gründe kommen wie rechtliche Anlässe, Erwartungen von Geschäftspartnern und Art und Weise der externen Datenlieferungen.

Die Bearbeitung der Frage, ob EDV für die Arbeitsschutzabteilung beschafft und eingeführt werden soll, ist in der Regel die Vorstufe zur Prämisse, dass EDV beschafft wird. Bei Vorhandensein zwingender externer und/oder außerökonomischer Anlässe zur Beschaffung von EDV kann von der Prämisse der EDV-Einführung ausgegangen werden. In vielen Fällen handelt es sich `nur´ um eine Anpassung und/oder Erweiterung des vorhandenen Systems. Aber auch in diesen Fällen sollte man sich mit obigen Fragen und Themen auseinandersetzen. Dies ist auch ein guter Anlass, eine Ist-Analyse des Arbeitsbereichs der Arbeitsschutzabteilung/ der Fachkraft für Arbeitsicherheit durchzuführen, falls das noch nicht aus anderem Anlass geschehen ist.

6.2 Systemanalyse

Die Ist-Analyse des Aufgabenbereichs und Aufbaus der Arbeitsschutzabteilung/des Aufgabenbereichs der Fachkraft für Arbeitssicherheit kann auch als Systemanalyse bezeichnet werden, so wie dies in der Organisationstechnik üblich ist./vgl. z.B. Hof. S. 133 ff./ Oft greift man auf die Resultate der Vorphase zurück, überprüft und ergänzt diese soweit es notwendig und/oder möglich ist. In vielen Fällen bietet sich für die Systemanalyse eine funktionsorientierte Vorgehensweise an. Man kann wieder die Aufgabenbeschreibung von Grassl/Sinks (Anhang 6-2) als Basis nehmen. Den Ausgangspunkt für die Beschreibung der Ergebnisse der Systemanalyse bilden die Arbeitsabläufe der Arbeitsschutzabteilung/der Fachkraft für Arbeitssicherheit wie sie aus der Aufgabenbeschreibung interpretiert werden können und die daraus ableitbaren Informationsfunktionen wie sie in Bild 6-1 dargestellt sind. Dies kann EDV-mäßig unterteilt werden in die Bereiche Daten-`input´ und Daten-`output´.

Die Funktionen, die neu- oder umgestaltet werden sollen, sind aus der 'Ist-Aufnahme' herauszufiltern und abzugrenzen. Die Hauptfunktionen sollen in Teilfunktionen zerlegt werden. Im Falle der Hauptfunktion `Unfallanalyse´ bedeutet dies beispielsweise die Zerlegung in die Teilfunktionen: `Unfalldaten

ermitteln´, `Unfalldaten eingeben´, `Unfalldaten be-/verarbeiten´, `Unfalldaten auswerten´ und 'Ergebnisse präsentieren'.

Zur Systemanalyse (Ist-Aufnahme) gehören ebenso:

- Formularanalysen (d.h. die Unfallanzeige nach BG, die Betriebsanweisung nach § 20 GefStoffV, die Sicherheitsdatenblätter nach TRGS 220 etc müssen unter dem Gesichtspunkt der EDV-mäßigen Weiterverarbeitung analysiert werden.)
- Datenanalysen (d.h. die Daten [Unfalldaten, Gefahrstoffdaten usw.] müssen dahingehend überprüft werden, was davon mit dem Rechner weiter verarbeitet werden kann bzw. muss.)
- Mengenanalysen der Daten (d.h. es muss überprüft werden, in welcher Menge die Daten anfallen - die wahrscheinliche Anzahl der Unfälle, die Anzahl der Gefahrstoffe usw. muss festgestellt oder angegeben werden.)
- Beschreibung der Datenflüsse wie es in Bild 6.1 grob dargestellt ist; d.h. es muss angegeben werden, wer von wem welche Daten empfängt und wer wem welche Daten weitergibt; z.B. Gefahrstoffdaten kommen vom Lieferanten zum Einkauf, von dort gelangen sie zum Arbeitsschutz und von da zum medizinischen Dienst.

	Datenquellen *Informations-input*	*Informations-datensenken*	Verarbeitung *Informations-output*	
Betriebs-abteilungen, medizinischer Dienst, Betriebsrat, Belegschaft, Personal-abteilung, Literatur, Forschung, Aufsichts-behörden, Berufsge-nossenschaft	Unfall-meldungen, Unter-suchungen bzw. Unter-suchungs-berichte, Vorschläge, Vorschriften, Em-pfehlungen, Kosten, Verfahren	Arbeits-schutzab-teilung bzw. Fachkraft für Arbeits-sicherheit	Unfall-anzeigen, Listen, Aus-wertungen, Vergleiche, Em-pfehlungen, Anweisungen, Merkblätter	Betriebs-abteilungen, medizinischer Dienst, Betriebsrat, Belegschaft, Personal-abteilung, Forschung, Aufsichts-behörden, Berufsge-nossenschaft, Unter-nehmens-leitung

Bild 6.1 Informationsumgebung einer Arbeitsschutzabteilung /Utt/

6.2.1 Istaufnahme (am Beispiel Unfalldaten)

Die in der Vorphase bereits aufgenommen Aufgaben werden hier in ihrer Art und Abwicklung beschrieben und in ihre einzelnen Elemente zerlegt. An dem Tätigkeitsbereich 'Unfalldatenerfassung und -verarbeitung' soll dies beispielhaft aufgezeigt werden.

Zur Unfalldatenerfassung können folgende Teiltätigkeiten gehören:

- Befragung des Beschäftigten, der den Unfall hatte – falls der dazu schon/ noch in der Lage ist. (Notizen machen!) Formblatt mit Standardfragen und/ oder Stichpunkten?
- Befragung der Zeugen, falls welche da sind. (Notizen machen!) Formblatt mit Standardfragen und/oder Stichpunkten?
- Analyse des Unfallgeschehens anhand einer Betrachtung der Unfallumgebung und der beteiligten Gegenstände. (Notizen/Photos machen!) Formblatt mit Standardfragen und/oder Stichpunkten?
- Mit dem/den behandelnden Ersthelfer/Sanitäter/Arzt sprechen. Formblatt mit Standardfragen und/oder Stichpunkten?
- Den Unfallbericht schreiben, betriebseigene Unfallmeldung ausfüllen.
- Die Unfallmeldung für den Unfallversicherungsträger ausfüllen und übermitteln.
- Wenn die Unfallursache technische (Sicherheits-) Mängel waren, muss ein Gespräch mit der Betriebsleitung zu diesem Thema stattfinden, insbesondere wenn man vorher schon erfolglos auf diese Mängel hingewiesen hat.
- Die Unfalldaten für die Unfallstatistik aufbereiten.
- Den Unfallbericht einige Zeit später mit den gemachten Notizen und Photos vergleichen – mögliche Ungereimtheiten abklären.

Zusätzlich müssen die verwendeten Formulare und Merkblätter auf folgende Punkte überprüft werden:

- Inhaltliche Aktualität
- Vollständigkeit
- Übereinstimmung mit offiziellen Formularen
- Gut und schnell ausfüllbar

6.2.2 Schwachstellenanalyse (am Beispiel Unfalldaten)

Bei der Unfalldatenerfassung und –verarbeitung war vor der „Computerzeit" und ist m.E. weiterhin der Mensch die Hauptschwachstelle. Man ist als FaSi darauf angewiesen, dass man von Unfallbeteiligten und Zeugen genaue Auskünfte bekommt. Ansonsten wird der Unfallbericht nicht genau und kann nicht erfolgversprechend für die Unfallursachenermittlung verwendet werden.

Die weitere Vorgehensweise nach der Befragung kann kaum zu Fehlern führen. Probleme können nur entstehen, wenn ein Anderer die handgeschriebenen Notizen verarbeiten und auswerten muss. (Problemmöglichkeiten sind das Lesen der Handschrift und die Interpretation des Inhaltes)

Die Probleme mit der Handschrift kann man vermeiden, wenn ein Maschinenschreibgerät mitgenommen wird – Laptops sind recht handlich und werden immer preisgünstiger und leistungsfähiger.

Es ist auch möglich, die verwendeten Formulare und Merkblätter erst in dieser Phase auf die obengenannten Punkte zu analysieren.

6.3 Zielfestlegung

"Die Zielfestlegung umfasst die kritische Überprüfung der Systembeschreibung und darauf aufbauend das Setzen globaler Informationsziele für das neue computergestützte Informationssystem." /Hof, S. 144/ Es muss in dieser Phase bestimmt werden, ob das zu beschaffende/zu ergänzende Programm nur bestimmte Aufgabenbereiche wie Unfalldatenerfassung und -bearbeitung oder Gefahrstoffverwaltung beinhalten soll oder ob dieses Programm beispielsweise eine sogenannte Komplettlösung sein soll. Sollen mehrere Anwender damit arbeiten, müssen deren Zielvorstellungen zusammengefasst werden.

6.4 Durchführbarkeitsstudie und Sollkonzeption

In der Regel werden Zielvorstellung und Durchführbarkeitsstudie und Sollkonzeption iterativ abwechselnd durchgeführt, bis zur abschließenden Sollkonzeption. In der Durchführbarkeitsstudie werden anhand wirtschaftlicher, technischer und organisatorischer Kriterien die gewünschten Zielvorstellungen überprüft. Nicht zu unterschätzen/vernachlässigen sind bei solchen Überprüfungen ergonomische Grundregeln sowie die Vorgaben zu Datenschutz und Datensicherheit. Das iterative Vorgehen ist demzufolge bei Eigenprogrammierung bedeutsam und bei Beschaffung von Software, die in wirtschaftlicher, technischer, organisatorischer Hinsicht und/oder aus Datenschutzgründen problematisch sein kann. Die Durchführbarkeitsstudie wird bei der Beschaffung von Software für den Arbeitsschutz keine allzu große Bedeutung haben, denn das Marktangebot ist so vielfältig, die Programme sind ergonomisch kaum noch zu beanstanden, dass es `nur´ eine finanzielle Frage ist, wieweit die Zielvorstellungen erfüllbar sind.
Aufbauend auf den Ergebnissen der Durchführbarkeitsstudie wird das Soll-konzept erstellt, das die Grundlage für das zu erstellende Pflichtenheft zum Systementwurf bzw. zum Einkauf des Systems bildet.

6.5 Systementwurf oder Systembeschaffung

Im Falle einer Neu- oder Umprogrammierung muss nun eine detaillierte Beschreibung erstellt werden, die Auskunft darüber gibt, was wie programmiert werden soll. Diese sogenannte Systemstrukturierung und der daraus erstellte Detailentwurf beinhalten u.a. eine Datenspezifikation, eine Schnittstellen-spezifikation und eine Programmspezifikation. Auch Vorgaben zum Testen der Software gehören zum Systementwurf.

Der Praktiker im Bereich Arbeitsschutz wird in der Regel nicht selbst programmieren, sondern die benötigte Software kaufen. Im Falle einer Beschaffung der Software wird der Kauf anhand der im Sollkonzept/im Pflichtenheft festgelegten Kriterien durchgeführt.

Spätestens jetzt stellt sich einer FaSi die Frage nach den Bezugsquellen der gewünschten Software.

"Einzelne Anschriften von Anbietern sind den Arbeitssicherheitszeitschriften aus Werbeanzeigen oder Berichten über derartige Software zu entnehmen. Es besteht auch die Möglichkeit, sich an den Verein Deutscher Sicherheitsingenieure (VDSI) zu wenden. Man kann davon ausgehen, dass dort ein Ansprechpartner sein wird, der Auskunft darüber geben kann, wo Anschriften der verschiedenen Anbieter zu finden sind.

Die so ermittelten Anbieter werden um Informationsmaterial über ihre Programme gebeten. Anhand der erhaltenen Informationen kann eine Grobauswahl getroffen werden, indem die offensichtlich nicht geeignete Software ausgeschlossen wird. Die in Frage kommenden Anbieter werden um ein Angebot auf der Grundlage des erstellten Pflichtenheftes gebeten. Anhand der Antworten auf diese Bitten lassen sich wiederum die Programme ausfiltern, die dem Anforderungsprofil am wenigsten entsprechen.

Die Anbieter, deren Produkte die Anforderungen des Pflichtenheftes am besten zu erfüllen scheinen, werden um Vorführung der Programme ersucht. Bei der Beurteilung der Software aufgrund einer Vorführung ist allerdings Vorsicht geboten, vor allem bei modular aufgebauten Programmen, da von den Vertriebsbeauftragten meistens nur die Module vorgeführt werden, die am leistungsfähigsten sind. Es sollte auf die Vorführung der gesamten Anwendungsmöglichkeiten der Software bestanden werden.

Die effizienteste Weise solch ein Produkt zu beurteilen, ist die Möglichkeit das gewünschte Programm im eigenen Hause auszutesten. Wenn also die Möglichkeit einer Probeinstallation gegeben ist, sollte diese auf jeden Fall in Anspruch genommen werden." /Wun, S. 6/

Da man meistens davon ausgehen muss, dass kein Programm den Idealan-forderungen genügt, wird man das Programm unter dem Gesichtspunkt aussuchen müssen, "auf welche Vorteile der einzelnen Programme im Grad der

Anforderungserfüllung der Bewertungskriterien am meisten Wert gelegt wird." /Wun, S. 7/

So trivial dies auch klingen mag: "bevor letztendlich ein Kaufvertrag abgeschlossen wird, ist er genau zu überprüfen. Dabei ist keine einzige Klausel außer acht zu lassen, denn auch der Inhalt eines solchen Vertrages kann als Entscheidungskriterium für die endgültige Wahl maßgebend sein. Hierbei sind insbesondere die Aspekte der Dienstleistungen (Anm.: Hotline, Notfallservice, Update etc.) und der Garantie in Betracht zu ziehen." /Wun, S. 7/

6.6 Systemimplementierung und Systembetrieb

Diese Phase umfasst je nach Gegebenheit die Programmierung anhand der Programmiervorgaben oder das Beschaffen und Einführen der Programme anhand der Vorgaben des Pflichtenheftes. Zusätzlich müssen Maßnahmen durchgeführt werden zur Schaffung der notwendigen organisatorischen Voraussetzungen für den Einsatz des Programmsystems.

Im Falle einer Eigenprogrammierung wird begleitend zur Programmierung eine Programmdokumentation erstellt, die es später ermöglichen soll, Wartungs- oder Erweiterungsarbeiten an Teilprogrammen durchführen zu können. Auch zur Erleichterung der Fehlersuche ist es notwendig, Unterlagen über intern verwendete Schlüssel, Tabellen, Programmiertricks und die Meldungen zu führen.

Ein Benutzerhandbuch ist bei einer Eigenprogrammierung ebenfalls zu erstellen; bei der Beschaffung eines Programms ist es i.d.R. im Lieferumfang enthalten. Es ist die Grundlage für die Schulung und die selbständige Arbeit der zukünftigen Anwender. Daher muss es Programmfunktionen, Formulare, Menümasken und Datenflüsse beschreiben, am besten in Anwendungsbeispielen erklären und Hinweise zur Erklärung von Fehlermeldungen geben. Im Falle einer Gefahrstoffdatenbank sollten u.a. die Angaben zu den Stoffen erläutert werden, die Sortierkriterien sollten aufgezählt und erläutert werden und die Eingabe- und Suchmöglichkeiten sollten erklärt werden. Hinweise zur Behebung (häufig) auftretender Fehler sollten ebenfalls enthalten sein. Nutzungsanweisungen für bestimmte Geräte, Arbeitsanweisungen für Datensicherung, Terminregelungen, Verteiler für Listen u.ä. müssen auch erstellt werden bzw. gehören normalerweise zum Lieferumfang.

Die zusätzlich durchzuführenden Maßnahmen beinhalten die Einrichtung der Arbeitsplätze, die Beschaffung von Hilfsmaterialien sowie die Installation von Geräten. Auch bei einer Ergänzung/Aktualisierung vorhandener Software wird es oft notwendig sein, neue Hardware zu beschaffen; dies ist auch oft ein guter Anlass, den Rechnerarbeitsplatz ergonomisch besser zu gestalten.

In der letzten Phase wird das Programm in der Praxis getestet. Aus diesem Test heraus können insbesondere bei Eigenprogrammierung letzte Änderungen

anfallen zur Vervollständigung, Bereinigung oder Änderung der Dokumentation und Detailkorrekturen am Programm. Aber auch beim Kauf können (je nach Vertrag) noch Ergänzungen und/oder Detailkorrekturen am Programm durchgeführt werden. Die Art der Einführung des Programms hängt u.a. ab von folgenden Faktoren:

⇒Neue Einführung von EDV

⇒Ergänzung von Hardware und Software

⇒Ergänzung nur von Software

⇒(Allgemeine) betriebliche Randbedingungen

Je nach diesen Randbedingungen erfolgt die Einführung schrittweise und parallel zur bisherigen Verfahrensweise, oder es erfolgt eine Umstellung zu einem bestimmten Zeitpunkt.

6.7 Marktüberblick

Das Marktangebot ist - entsprechend dem Aufgabenbereich einer FaSi - sehr umfangreich. Es werden für alle Tätigkeitsbereiche, die mit Hilfe von EDV bearbeitet werden können, fertige, d.h. sofort einsetzbare Softwarelösungen angeboten. Oft werden auch sogenannte Tools angeboten, d.h. Softwarelösungen, die auf marktübliche Standardprogramme aufgesetzt werden können und (etwas) Nachbearbeitung/Anpassung benötigen. Das Angebot reicht von Software, welche ein einzelnes Problem bearbeiten (z.B. Betriebsanweisungen erstellen) bis hin zu sogenannten Komplettlösungen, in denen versucht wird das ganze Aufgabenfeld einer FaSi abzudecken. In verschiedenen Marktübersichten hatte sich gezeigt, dass gefahrstoffbezogene Software einen sehr großen Marktanteil hat. H. Wunenburger sprach von einem cirka zweidrittel Anteil./Wun/ Mit gefahrstoffbezogenen Software werden i.allg. folgende Unterbereiche bearbeitet:

- Gefahrstoffverwaltung
- Gefahrstoffkennzeichnung
- Gefahrstoffkatastererstellung
- Betriebsanweisungen (Erstellung)
- Sicherheitsdatenblätter (Erstellung)
- Unfallmerkblätter (Erstellung)
- Arbeitsbereichsanalysen
- Messdatenverarbeitung
- Ermittlungsverfahren
- Gefahrguttransport

In manchen Programmen, die sich mit die Gefahrstoffproblematik als Thema befassen sowie bei sogenannten „Komplettlösungen“ werden auch umweltschutzspezifische Elemente mit angeboten:

- Gewässerschutz
- Abfallmanagement
- Abfallentsorgung
- Immissionsschutz
- Emissionsschutz

Weitere, oft eigenständige Programme, die einer FaSi als Arbeitsmittel dienen können, gibt es für folgende Tätigkeitsbereiche:

- Arbeitsschutz
- Umweltschutz
- Arbeitsmedizin
- Strahlenschutz
- Brandschutz
- Werkschutz

Ganz generell werden noch Programme zur Termin- und Literaturverwaltung sowie zum Mahnwesen und Symbolbibliotheken angeboten. Unter dem Thema Arbeitsschutz finden sich Programme zur Unfalldatenerfassung und –bearbeitung, zur Anlagen-, Maschinen- und Arbeitspatzüberwachung, zur Verwaltung der persönlichen Schutzausrüstung sowie zur Erstellung von Arbeitsanweisungen und Sicherheitsvorschriften.

6.7.1 Komplettlösungen

Auf dem Markt werden verschiedene betriebliche Arbeits- und Umweltschutzmanagementsysteme mit Fachanwendungen aus den Bereichen Arbeitssicherheit und Umweltschutz angeboten. Diese Programme sind modular aufgebaut. „Durch den modularen Aufbau können die Fachanwendungen individuell eingesetzt und jederzeit erweitert werden.“ /GUB/

Als Philosophie liegt diesen Programmen zugrunde, dass in der betrieblichen Realität Arbeits- und Umweltschutz nur noch gemeinsam effizient bewältigt werden können. GUB wirbt beispielsweise für WAUplus folgendermaßen:

„WAUplus ist die Standardlösung für alle Kernbereiche des Arbeits- und Umweltschutzes im Unternehmen. Praxisgerechter Informationsverbund und Vollzugsoptimierung in einem, für

- Abfallmanagement
- Gefahrstoffmanagement
- Gefahrgutmanagement

- betrieblichen Arbeitsschutz
- betriebliche Unfallbearbeitung
- Gefahrenabwehr
- Anlagenverwaltung.

Mit WAUplus und seinen breiten Auswertungsmöglichkeiten bis hin zu automatischen Behördenberichten bündeln Sie Ihre Betriebsdaten auf Abruf zu planungs- und kontrollrelevanter Information.“/GUB/

Diese Programme sollen Routinetätigkeiten vereinfachen, die dezentral verteilten Daten im Unternehmen strukturierten und so die notwendige Transparenz bei der Aufgabenerfüllung schaffen. GUB schreibt dazu:

„WAUplus ist IT-Unterstützung mit Mehrwert von Anfang an, durch

- Erhöhung der Rechtssicherheit
- automatisches Erstellen der gesetzlichen vorgeschriebenen Behördenberichte
- mehr Wirtschaftlichkeit durch verringerte Zeit- und Personalaufwände
- Verringerung der Pflegeaufwände durch integrierte Datenbestände
- Erstellung von Datensichten für Anwender, Vorgesetzte und Management
- verbessertes Controlling auf der Grundlage von Auswertungen über beliebige Datenzusammenhänge

Es unterstützt die Aufgabenträger aus den Bereichen Arbeits- und Umweltschutz in Industrie und Gewerbe bei der einheitlichen Umsetzung der gesetzlichen Auflagen.“/GUB/

Die Hersteller dieser immer noch recht kostenintensiven Software sind natürlich darum bemüht softwaretechnisch auf dem neuesten Stand zu sein und den Anwendungskomfort und –nutzen hoch zu halten. Die meisten dieser Programme sind Windows angepasst und daher für den Windows Nutzer gut anzuwenden. Noch einmal das Beispiel GUB:

„Die folgenden Eigenschaften von WAUplus gewährleisten sowohl eine schnelle Erlernbarkeit der Anwendung, als auch eine hohe Leistungsfähigkeit des Gesamtsystems:

- graphische Benutzeroberfläche
- verfahrensübergreifende Strukturierung der einzelnen Bildschirmmasken
- durchgängige Mausunterstützung

- Aufteilung der Anwendung in verfahrensübergreifende (Termine, Kataloge, Phrasen, Adressen,...) und verfahrensspezifische Komponenten (Unfallbearbeitung, Kreislaufwirtschaftsgesetz, Arbeitsschutz,...)
- Integrationsmöglichkeit von Bürokommunikationssystemen (Excel, Winword) und
- Geoinformationssystemen (SICAD Spatial Desktop).
- verfügbar in Client/Server-Architektur oder als Stand-alone-System.
- WAUplus kann auf verschiedenen HW-Plattformen einpasst werden (Konditionen erhalten Sie auf Anfrage)."/GUB/

Wie GUB betont und selbstverständlich auch für alle anderen Hersteller gilt, ist die Grundlage für die Entwicklung der einzelnen Module – GUB spricht von Bausteinen - dieser Programme bundeseinheitliche Gesetze und Verordnungen. Änderungen und Erweiterungen in den Rechtsvorschriften werden in den entsprechenden Fachanwendungen berücksichtigt. Mit der Herausgabe neuer Programmversionen versuchen die Hersteller für eine möglichst rasche Anpassung an neue und/oder geänderte Rechtsvorschriften zu sorgen.

6.7.2 Arbeitsschutzprogramme

Unter dem Stichwort „Arbeitsschutzprogramme" wird in der Regel „Unfalldatenerfassungs- und –bearbeitungsprogramme" verstanden. In Kapitel 8 wird auf die gesetzlichen, softwaretechnischen und statistischen Grundlagen solcher Programme eingegangen.

Programme in diesem Verständnis ermöglichen die Aufnahme der Unfalldaten wie es für Unfallmeldungen an die Versicherungsträger notwendig ist. Es ist oft so, wenn ein Zugriff auf Personaldaten (Diskette, Netz) möglich ist, dass die persönlichen Daten des Verunfallten direkt eingelesen werden können. Dadurch kann die Schreibarbeit deutlich verringert werden. Die Unfallmeldungen können entsprechend der Anforderungen des Versicherungsträgers und/oder anderer Stellen ausgedruckt werden. Für die in der Regel möglichen statistischen Auswertungen können die Daten von den persönlichen Daten gelöst werden, bzw. die Daten können kodiert werden. Entweder bieten die einzelnen Programme eine Schnittstelle zu marktgängigen Statistikprogrammen oder sie bieten eigene statistische und graphische Funktionen, die eine Auswertung mindestens nach den üblichen Kriterien des Unfallverhütungsberichtes der Bundesregierung ermöglichen. Diese Statistiken sollen der Unfallursachenforschung dienen, Unfallschwerpunkte und Gefahrstellen sollen so ermittelt werden. Einige Hersteller bieten auch eine Möglichkeit zur Verfolgung des Einzelfalles bis zum endgültigen Abschluss und bieten Standardbriefe für die

notwendige Korrespondenz. Zusätzlich können verschiedene Programme die Unfallkosten (zumindest grob) berechnen.
In den Rahmen dieser Software gehören auch Programme, die das Verbandsbuch ersetzen. Hier werden die „Erste Hilfe“ Leistungen eingetragen. Die angebotenen möglichen Eintragungen reichen von dem gesetzlichen Mindesteintrag bis hin zu einem für Unfallforschungszwecke geeigneten Eintragungsschema.

6.7.3 Gefahrstoffbezogene Software

Unter dem Begriff „Gefahrstoffbezogene Software“ werden betriebliche Arbeits- und Informationssysteme für eine sichere Hantierung von Gefahrstoffen verstanden. Darunter fallen reine Gefahrstoffdatenbanken, Programme zur Erstellung von Sicherheitsdatenblättern und Betriebsanweisungen, zur Erstellung von Gefahrstoffetiketten und zur Gefahrstoffkennzeichnung. In Kapitel 7 werden die notwendigen theoretischen Grundlagen beschrieben, die zur Anwendung dieser Software Voraussetzung sind. Auch Programme, die sich mit der Abfallproblematik befassen, fallen unter diesen Begriff.

Programme, die sich mit dem Thema Abfall befassen bieten in der Regel folgende Inhalte:

- Datenbankfunktionen
    - Gefahrstoffe
    - Abfälle
    - Erzeuger
    - Entsorger
    - Verwerter
- Lieferscheinerstellung
- Amtliche Formulare
- Statistische Auswertungen
- Kostenrechnung

Gefahrstoffprogramme offerieren oft:

- Gefahrstoffdaten oder/und
- Speicherung und Verwaltung von Gefahrstoffdaten
- Erstellung eines Gefahrstoffkatasters

- Erstellung von Sicherheitsdatenblättern
- Erstellung von Betriebsanweisungen
- Erstellung von Gefahrstoffetiketten

Normalerweise sind diese Programme modular aufgebaut.

Es gibt auch reine Gefahrstoffdatenbanken wie z.B. Kühn Biretts gelbe Seiten für PC oder Sorbe für PC. Ebenso für die anderen Aufgaben wie das Erstellen von Betriebsanweisungen oder Sicherheitsdatenblätter gibt es eigene Programme. Kleine Hilfsprogramme stellen Symbolbibliotheken, R- und S-Sätze sowie deren Kombinationen zur Verfügung. Am Beispiel von BETRAN wird der Leistungsstand und der technische Stand dieser (Zusatz-)Programme beschrieben:

„BETRAN ist ein Programm zur Erstellung von:

- Betriebsanweisungen gemäß § 20 GefStoffV
- Sicherheits-Betriebsanweisungen (z.B. gemäß UVV)
- Umweltschutzanweisungen
- Führung eines Gefahrstoffkatasters nach § 12 GefStoffV

Allgemeine Informationen

Die Steuerung aller Funktionen erfolgt über eine eigene Symbolleiste in Word, die frei positioniert werden kann. BETRAN basiert auf einer Access 2.0 kompatiblen Datenbank, in der alle relevanten Informationen abgelegt werden. Dadurch können z.B. Informationen aus bereits bestehenden Gefahrstoffdateien ohne große Probleme in BETRAN importiert werden. BETRAN wird mit einem Access Runtime-Modul geliefert, d.h. Microsoft Access ist nicht zum Einsatz erforderlich. Die erstellten Betriebsanweisungen werden als Word-Dateien abgelegt.

Erstellung von Betriebsanweisungen

Die Formatierung der einzelnen Textpassagen kann frei gewählt werden. Symbole können wahlweise in jeden Abschnitt eingefügt werden. Die Symbole werden jeweils kontextsensitiv mit Grafikvorschau angezeigt. Dadurch wird die Benutzung deutlich vereinfacht.

Das Gefahrstoffverzeichnis

BETRAN verwaltet Gefahrstoffe arbeitsplatzbezogen, d.h. die Gefahrstoffe und Stoffmengen werden Arbeitsplätzen zugeordnet, die in der Standortdatei verwaltet werden. Es stehen Standardreporte zur Verfügung, die alle Informationen in übersichtlicher Form darstellen.

Einbindung der Standardtext-Verwaltung sowie R- und S-Sätze

R- und S- Sätze wurden aufgenommen und können über entsprechende Dialoge eingefügt werden. Die Standardtextverwaltung ist vollständig in BETRAN integriert. Sie können auch eigene Textkategorien und Themenbereiche anlegen.

Symbole und Symbolverwaltung

Über den integrierten Symbolmanager können Sie auf die Symbole nach Themenbereichen sortiert zugreifen.

BETRAN enthält alle im Arbeitsschutz relevanten Symbole. Die 250 enthaltenen Symbole entstammen den folgenden Gruppen:

Gefahrstoffe, Verbote, Gebote, Rettung/Brandschutz, Erste Hilfe, GGVS Zeichen, Warnhinweise, Entsorgung

Alle Symbole sind als Vektorgrafik (WMF) enthalten, dadurch ist beliebige Skalierung und Ausdrucke in jeder Größe ohne Qualitätsverlust möglich."/JMV/

Es ist auch möglich, einige der genannten Aufgaben sich mit Hilfe von über das Internett \`online´ (man arbeitet mit einem anderswo gelagerten Programm als ob es auf dem eigenen Rechner wäre) erreichbaren Programmen zu erleichtern. Natürlich hat solche Internettsoftware den Nachteil, dass die Bearbeitungszeit größer ist und wenn man z.B. auf eine Gefahrstoffdatenbank oft zugreifen muss, fangen auch die Telefonkosten an, bemerkbar zu werden. Wenn es jedoch nicht allzu oft notwendig ist, Gefahrstoffdaten nachzuschauen, sollte man sich überlegen, ob man – statt eine Datenbank zu kaufen – auf eine Datenbank wie GESTIS über das Internett zugreift:

„GESTIS-Stoffdatenbank

Gefahrstoffinformationssystem der gewerblichen Berufsgenossenschaften

Inhalte

Die GESTIS-Stoffdatenbank enthält Informationen für den sicheren Umgang mit chemischen Stoffen am Arbeitsplatz, wie z.B. die Wirkungen der Stoffe auf den Menschen, die erforderlichen Schutzmaßnahmen und die Maßnahmen im Gefahrenfall (inkl. Erste Hilfe). Darüber hinaus wird der Nutzer über wichtige physikalisch-chemische Daten der Stoffe sowie über spezielle gesetzliche und

berufsgenossenschaftliche Regelungen zu den einzelnen Stoffen informiert. Es sind Informationen zu etwa 7000 Stoffen enthalten. Die Pflege der Daten erfolgt zeitnah nach Veröffentlichung im Vorschriften- und Regelwerk oder nach Vorliegen neuer wissenschaftlicher Erkenntnisse. Die GESTIS-Stoffdatenbank kooperiert mit der Gefahrstoffdatenbank der Arbeitsschutzbehörden der Länder (GDL).

Nutzung

Der Datenbestand darf zum Zwecke des Arbeitsschutzes bzw. zur Informationsgewinnung über die von chemischen Stoffen ausgehenden Gefährdungen genutzt werden. Eine kommerzielle Nutzung der Daten wie auch eine teilweise oder vollständige Übernahme in andere Informationssysteme ist nicht gestattet."/GES/

7 Gefahrstoffprogramme

Wie schon in Kapitel 6 erwähnt zeigen verschiedene Marktübersichten (vgl. Wun, Har), dass man als FaSi in diesem Bereich die größte Auswahl an Software hat. H. Wunenburger sprach von einem 2/3 Anteil am Gesamtangebot der Software, die für eine FaSi interessant ist./Wun, S.9/ Die Nachfrage nach solchen Programmen ist relativ groß. Dies liegt daran, dass in fast jedem Betrieb Gefahrstoffe vorhanden sind und verwendet werden. Oft ist deren Menge groß, so dass es problematisch ist, diese manuell zu verwalten. Auch die Vielzahl der Stoffe machen solche Programme lohnenswert. Zu dieser Nachfrage hat aber auch das sehr komplexe Gefahrstoffrecht beigetragen. Hinzu kommt, dass solche Programme von erfahrenen Softwareherstellern relativ `einfach´ hergestellt werden können. Die Anwendungsmöglichkeiten dieser Programme sind vielfältig und umfassen generell alle Punkte, die vom Gefahrstoffrecht vorgeschrieben werden und per EDV durchführbar sind:

⇒“Gefahrstoffverwaltung

⇒Erstellen von Sicherheitsdatenblättern

⇒Arbeitsbereichsanalysen

⇒Ermittlungsverfahren

⇒Erstellen von Gefahrstoffkataster

⇒Erstellen von Unfallmerkblätter

⇒Messdatenbearbeitung

⇒Gefahrstoffkennzeichnung

Bei der gefahrstoffbezogenen Software wird oft auch das Gebiet “Umweltschutz” mit einbezogen. Dabei handelt es sich um die Themen Gewässerschutz, Gefahrgut, Abfallmanagement/Abfallentsorgung, Immissionsschutz und Emmissionsschutz.” /Wun, S. 10/

7.1 Gefahrstoffrecht

Das deutsche Gefahrstoffrecht gilt als eines der schärfsten und restriktivsten Gefahrstoffrechte in der Welt. Dies ist aber auch notwendig in einem Land, dass so dicht besiedelt ist wie Deutschland, in dem so viele chemische Betriebe angesiedelt sind und wo so viele verschiedene Chemikalien benutzt werden.

Grundlage des Gefahrstoffrechtes ist das Chemikaliengesetz. Darauf begründet sich die Gefahrstoffverordnung und diese ist wiederum Grundlage der technischen Regeln für Gefahrstoffe.

7.1.1 Gefahrstoffverordnung

“Zweck der Gefahrstoffverordnung ist der Schutz des Menschen vor arbeitsbedingten und sonstigen Gesundheitsgefährdungen sowie der Schutz der

Umwelt vor stoffbedingten Schädigungen beim Umgang mit Gefahrstoffen. Gefahrstoffe als solche sind in ihrer Art und Größe bestehende und nicht zu verändernde Gefährdungsquellen, deren Gefährdungs-potential nur durch Schutzmaßnahmen limitiert und/oder reduziert werden kann. Die in der Gefahrstoffverordnung geforderten Schutzmaßnahmen … dienen ... der Gefährdungsbegrenzung bzw. der Schädigungsabwehr. ...”/Nie, S. 44/
Im Rahmen dieses Buches werden die §§ 14, 20 und der Anhang 1 der Gefahrstoffverordnung besprochen, weil insbesondere diese Punkte in vielen Programmen realisiert wurden. Die Kenntnis der anderen Forderungen der Gefahrstoffverordnung sind für eine FaSi jedoch wichtig und teilweise wurden diese (soweit per EDV möglich) in einzelnen Programmen realisiert. Daher ist im Anhang dieses Buches im Internettverzeichnis eine Adresse angegeben, wo sich eine Version dieses Gesetzes findet. Dort sind auch R- und S-Sätze sowie die Gefahrensymbole und -bezeichnungen nachlesbar.
In § 14 und Anhang 1 Nr. 5 werden die Erstellung eines Sicherheitsdatenblattes gefordert und der Aufbau eines derartigen Blattes beschrieben. Solch ein Sicherheitsdatenblatt ist jedem gewerblichen Benutzer kostenlos in Deutsch (bzw. wenn ins Ausland geliefert wird, in seiner Landessprache) zur Verfügung zu stellen. Falls das Blatt aufgrund neuer Informationen und Erkenntnisse überarbeitet wurde, ist diese Version jedem Abnehmer der letzten 12 Monate zu übermitteln. Das Sicherheitsdatenblatt soll Auskunft geben über:

⇒die chemische Summenformel,
⇒die Gefahrenklasse,
⇒die Pack-Kategorie,
⇒die Lagerklasse,
⇒die entsprechenden R- und S-Sätze,
⇒den MAK oder TRK-Wert,
⇒die Gefahrenhinweise,
⇒sowie die Zuordnungsnummern (UN-Nummer, EG-Nummer, IATA/-CAO-Nummer usw.).

In § 20 wird die Erstellung einer Betriebsanweisung gefordert. Hierin muss auf die Gefahren für Mensch und Umwelt deutlich hingewiesen und die entsprechenden Schutzmaßnahmen und Verhaltensregeln festgelegt werden. Erste Hilfe Anweisungen und Verhaltensregeln für den Gefahrenfall sind ebenfalls unverzichtbare Bestandteile einer Betriebsanweisung. Die Betriebsanweisung muss verständlich sein und in der Sprache der Beschäftigten formuliert werden. Sie muss an geeigneter Stelle in der Arbeitsstätte ausgehängt werden. Auch hier ist im Anhang ein Beispiel zu finden.

7.1.2 Technische Regeln für Gefahrstoffe

Die Ausführungsbestimmungen der Gefahrstoffverordnung werden als "Technische Regeln für Gefahrstoffe (TRGS)" bezeichnet. Sie sind die detaillierten Anleitungen zur Umsetzung der Forderungen des Chemikaliengesetzes, der Gefahrstoffverordnung und anderer Gesetze aus diesem Umfeld. Der Stand der sicherheitstechnischen, arbeitsmedizinischen, hygienischen und arbeitswissenschaftlichen Anforderungen an den Umgang mit gefährlichen Stoffen soll hier widerspiegeln. Sie werden vom "Ausschuss für Gefahrstoffe" erstellt und formuliert. Der Bundesminister für Arbeit und Sozialordnung sowie der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit veröffentlichen diese im Bundesarbeitsblatt bzw. im Bundesgesundheitsblatt. In der TRGS 300 wird das Ziel dieser technischen Regel(n) wie folgt ausgedrückt:
"... Die Zielrichtung dieser TRGS ist der Arbeitsschutz im Sinne der Gefahrstoffverordnung. Die für die Sicherheit der Beschäftigten zu treffenden Maßnahmen können jedoch in Teilbereichen gleichzeitig dem Schutz der Nachbarschaft dienen. ..." /TRGS 300/
In den einzelnen technischen Regeln wird das gefährdungsfreie Arbeiten mit einzelnen Stoffen und Stoffgruppen in verschiedenen Situationen beschrieben. In der TRGS 200 zum Beispiel sind Methoden zur Einstufung und Kennzeichnung von (gefährlichen) Stoffen und Zubereitungen beschrieben. In der TRGS 220 beispielsweise wird der Aufbau und Inhalt eines Sicherheitsdatenblattes geregelt. Die TRGS 222 gibt die Einteilung der Gefahrstoffe wieder. In den TRGS 514 und 515 wird beschrieben wie gefährliche Stoffe gelagert werden und ein Lagerbrand in solch einem Gefahrstofflager verhindert werden kann. Schließlich werden in der TRGS 555 die Inhalte und Anforderungen einer Betriebsanweisung in ihren Einzelheiten festgelegt.

7.2 Wichtige Termini zum Thema Gefahrstoffe

Im Gefahrstoffrecht als auch bei der sonstigen Arbeit mit Gefahrstoffen werden verschiedene Termini benutzt, deren Kenntnis von jeder FaSi erwartet wird und deren Kenntnis auch in den Gefahrstoffprogrammen vorausgesetzt wird. Die wohl wichtigsten Termini werden hier in ihren Definitionen wiedergegeben. Wie sie ermittelt und verwendet werden, wird hier nicht beschrieben, wenn es nicht aus der Definition ersichtlich ist. Dies, um nicht zu sehr das eigentliche Thema des Buches zu verlassen.

7.2.1 MAK-, TRK- und BAT-Wert

"Der MAK-Wert (Anm.: **m**aximale **A**rbeitsplatz **K**onzentration) gibt die höchstzulässige Konzentration eines Gases, Dampfes oder Schwebstoffes in der

Luft am Arbeitsplatz an, die nach gegenwärtigem Stand der Erkenntnis bei wiederholter und langfristiger, in der Regel 8-stündiger Exposition bei 40 Stunden Wochenarbeitszeit im Durchschnitt von 4 aufeinanderfolgenden Wochen als unbedenklich angesehen wird. Der MAK-Wert wird in der Regel über Zeiträume bis zu einem Arbeitstag integriert. Nach dieser Definition ist eine kurzfristige Überschreitung des MAK-Wertes möglich. Je nach Gefährdungspotential des Stoffes darf diese Überschreitung jedoch bestimmte Zeitspannen sowie bestimmte Spitzenbegrenzungen (2 bis 10 Fache des MAK-Wertes) nicht überschreiten. Ist die wöchentliche Arbeitszeit kürzer als 40 Stunden, so gilt nur die Spitzenbegrenzung. Der MAK-Wert wird in ml/m^3 (äquivalent dazu ist die Einheit ppm = parts per million) oder in mg/m^3 angegeben. Der in ppm angegebene Wert kann durch Multiplikation mit dem Ausdruck Molgewicht/24 in mg/m^3 umgerechnet werden (gilt für 20 Grad C und 1013 hPa).
Da für Karzinogene nach gegenwärtiger Erkenntnis keine beliebig kleine als unbedenklich anzusehende Konzentration definiert werden kann, erfolgt die Vorgabe einer Grenzkonzentration hier durch die **t**echnische **R**icht**k**onzentration (TRK): Die Einhaltung des TRK-Wertes soll das Risiko einer Beeinträchtigung der Gesundheit mindern, ohne dies völlig ausschließen zu können. Er ist als Anhaltspunkt für zu treffende Schutzmaßnahmen zu werten und sollte bei gegebenen technischen Möglichkeiten möglichst weit unterschritten werden." /CSD/ Nach GefStoffV § 15 Abs. 6 sollen die Werte angegeben werden, die nach dem Stand der Technik erreicht werden können. Für die Expositionsdauer gelten die gleichen Bedingungen wie bei den MAK-Werten.
"Der BAT-Wert (**B**iologischer **A**rbeitsstoff-**T**oleranz-Wert) ist die beim Menschen höchst zulässige Quantität eines Arbeitsstoffes bzw. Arbeitsstoffmetaboliten oder die dadurch ausgelöste Abweichung eines biologischen Indikators von seiner Norm, die nach dem gegenwärtigen Stand der wissenschaftlichen Kenntnis im allgemeinen die Gesundheit des Beschäftigten auch dann nicht beeinträchtigt, wenn sie durch Einflüsse des Arbeitsplatzes regelhaft erzielt wird ..." /DFG, S. 83/ Für die Expositionsdauer gilt das Gleiche wie bei den MAK-Werten. Die BAT-Werte "werden ... in der Regel für Blut oder Harn aufgestellt." /DFG, S.83/

7.2.2 LD und LC-Werte

"LDLo
(Lethal Dose Low) Diejenige niedrigste Dosis, bei der durch irgendeine Applikation (außer durch Inhalation) Todesfälle bei Mensch oder Tier bekannt sind.
LCLo
(Lethal Concentration Low) Diejenige geringste Konzentration der Substanz in der Atemluft, bei der bei Mensch oder Tier Todesfälle auftreten.
LD50
(Lethal Dose Fifty) Diejenige Menge (Dosis) eines Stoffes, die bei irgendeiner Applikationsart (außer durch Inhalation) zum Tode von 50 % der Versuchstiere führt.
LC50
(Lethal Concentration Fifty) Diejenige Konzentration eines Stoffes in der Atemluft, die zum Tode von 50 % der über eine bestimmte Zeitspanne exponierten Versuchstiere führt. Zusätzlich zur Atemluftkonzentration ist hier also auch immer die Expositionsdauer anzugeben. Zur Einstufung der Inhalationsgefahr schreibt die Gefahrstoffverordnung eine Expositionsdauer von 4 Stunden vor." /CSD/

7.2.3 Fruchtschädigender Stoff

"Unter Fruchtschädigung wird die Schädigung der Entwicklung ungeborener Kinder verstanden. Das berühmteste Beispiel für einen derartigen Stoff war das Medikament CONTERGAN. Die Einstufung nach § 1.4.2.3 GefStoffV Anhang 1 entspricht der Richtlinie 67/548/EWG und ist damit eine europäische Festlegung. Es bedeuten:

Kategorie 1

Stoffe, die beim Menschen bekanntermaßen fruchtschädigend wirken. Es sind hinreichende Anhaltspunkte für einen Kausalzusammenhang zwischen der Exposition einer schwangeren Frau gegenüber dem Stoff und schädlichen Auswirkungen auf die Entwicklung der direkten Nachkommenschaft vorhanden.

Kategorie 2

Stoffe, die als fruchtschädigend angesehen werden sollten. Es bestehen hinreichende Anhaltspunkte zu der begründeten Annahme, dass die Exposition einer schwangeren Frau gegenüber dem Stoff zu schädlichen Auswirkungen auf die Entwicklung der Nachkommenschaft führen kann. Diese Annahme beruht im allgemeinen auf Tierversuchen und/oder sonstigen relevanten Informationen.

Kategorie 3

Stoffe, die wegen möglicher fruchtschädigender Wirkung beim Menschen Anlass zur Besorgnis geben. Aus geeigneten Tierversuchen liegen einige Anhaltspunkte vor, die jedoch nicht ausreichen, um den Stoff in Kategorie 2 einzustufen." /CSD/

7.2.4 Krebserregend

"Die Einstufung nach § 1.4.2.3 GefStoffV Anhang 1 entspricht der Richtlinie 67/548/EWG und ist damit eine europäische Festlegung. Es bedeuten:

Kategorie1

Stoffe der Kategorie 1 wirken beim Menschen bekanntermaßen krebserzeugend. Es sind hinreichende Anhaltspunkte für einen Kausalzusammenhang zwischen der Exposition eines Menschen gegenüber dem Stoff und der Entstehung von Krebs vorhanden.

Kategorie 2

Stoffe der Kategorie 2 sollten für den Menschen als krebserzeugend angesehen werden. Es bestehen hinreichende Anhaltspunkte zu der begründeten Annahme, dass die Exposition eines Menschen gegenüber dem Stoff Krebs erzeugen kann. Diese Annahme beruht im allgemeinen auf Langzeitversuchen und/oder sonstigen relevanten Informationen.

Kategorie 3

Stoffe der Kategorie 3 geben wegen möglicher krebserzeugender Wirkung beim Menschen Anlass zur Besorgnis. Genügend Informationen für eine befriedigende Beurteilung liegen jedoch nicht vor. Aus geeigneten Tierversuchen liegen einige Anhaltspunkte vor, die jedoch nicht ausreichen, um den Stoff in Kategorie 2 einzustufen." /CSD/

7.2.5 R-Sätze

Die Hinweise auf die besonderen Gefahren eines Stoffes werden als R-Sätze bezeichnet. "In dem (laufend aktualisierten) Anhang I der Richtlinie 67/548/EWG des Rates vom 16.8.1967 sind derzeit gut 2000 Chemikalien mit allen erforderlichen R-Sätzen aufgeführt. Deren Kennzeichnung ist damit gewissermaßen amtlich und muss daher stets in der angegebenen Form verwendet werden (sog. "Legaleinstufung"). Stoffe, die noch nicht nach dieser Richtlinie eingestuft sind, sind aufgrund eigener Erkenntnisse des Herstellers/Nutzers zu kennzeichnen (sog. "Selbsteinstufung"). Da die einzelnen Hersteller dabei nicht selten zu unterschiedlichen Ergebnissen kommen, erklärt dies, weshalb es bei der Kennzeichnung von Chemikalien gelegentlich Abweichungen geben kann. Die Definition über die Zuteilung von R-Sätzen ist im Anhang I der Gefahrstoffverordnung geregelt." /CSD/

7.2.6 S-Sätze

Die Vorschläge/Vorschriften zum gefährdungsfreien Umgang mit gefährlichen Stoffen sind als S-Sätze bekannt. "In dem (laufend aktualisierten) Anhang I der Richtlinie 67/548/EWG des Rates vom 16.8.1967 sind derzeit gut 2000 Chemikalien mit allen erforderlichen S-Sätzen aufgeführt. Deren Kennzeichnung ist damit gewissermaßen amtlich und muss daher stets in der angegebenen Form verwendet werden (sog. "Legaleinstufung"). Stoffe, die noch nicht nach dieser Richtlinie eingestuft sind, sind aufgrund eigener Erkenntnisse des Herstellers/Nutzers zu kennzeichnen (sog. "Selbsteinstufung"). Da die einzelnen Hersteller dabei nicht selten zu unterschiedlichen Ergebnissen kommen, erklärt dies, weshalb es bei der Kennzeichnung von Chemikalien gelegentlich Abweichungen geben kann. Die Definition über die Zuteilung von S-Sätzen ist im Anhang I der Gefahrstoffverordnung geregelt." /CSD/

7.3 In den meisten Programmen verwendete Klassifizierungen

In der Gefahrstoffverordnung, den Technischen Regeln für Gefahrstoffe und in europäischen Richtlinien werden verschiedene Klassifizierungen der Stoffe vorgeschlagen/vorgeschrieben. Diese orientieren sich nach Stoffeigenschaften generell, Lagerung und Verwendung sowie den Transportbedingungen.

7.3.1 Gefahrenkennzeichnung

"In dem (laufend aktualisierten) Anhang I der Richtlinie 67/548/EWG des Rates vom 16.8.1967 sind derzeit gut 2000 Chemikalien mit allen erforderlichen Warnsymbolen aufgeführt. Deren Kennzeichnung ist damit gewissermaßen amtlich und muss daher stets in der angegebenen Form verwendet werden (sog. "Legaleinstufung"). Stoffe, die noch nicht nach dieser Richtlinie eingestuft sind, sind aufgrund eigener Erkenntnisse des Herstellers/Nutzers zu kennzeichnen (sog. "Selbsteinstufung"). Da die einzelnen Hersteller dabei nicht selten zu unterschiedlichen Ergebnissen kommen, erklärt dies, weshalb es bei der Kennzeichnung von Chemikalien gelegentlich Abweichungen geben kann. Die Definition über die Zuteilung von Warnsymbolen ist im Anhang I der Gefahrstoffverordnung geregelt." /CSD/

Die verwendeten Kennbuchstaben bedeuten:

C: *Ätzend*
E: *Explosionsgefährlich*
F: *Leichtentzündlich*
F+: *Hochentzündlich*
O: *Brandfördernd*
T: *Giftig und/oder krebserzeugend (Zutreffendes ist anzugeben.)*
T+: *Sehr giftig*

Xi: *Reizend*
Xn: *Mindergiftig (Frühere Bedeutung: Gesundheitsschädlich) und/oder Verdacht auf krebserzeugend (Zutreffendes ist anzugeben.)*
N: *Umweltgefährlich*

7.3.2 Pack-Kategorie

“Die Gefahrgutverordnung Straße (GGVS) schreibt vor, dass gefährliche Güter der Klassen 3, 6.1 und 8 nur dann zusammengepackt werden dürfen, wenn sie nicht gefährlich miteinander reagieren können. Gefährliche Reaktionen im Sinne der GGVS sind:

⇒eine Verbrennung und/oder eine Entwicklung beträchtlicher Wärme;

⇒die Entwicklung von entzündbaren und/oder giftigen Gasen;

⇒die Bildung von ätzenden flüssigen Stoffen;

⇒die Bildung instabiler Stoffe.

Die Frage, ob eine der hier beschriebenen gefährlichen Reaktionen zwischen verschiedenen Stoffen der genannten Klasse auftreten kann, ist geprüft und das Ergebnis dieser Prüfung in einem Zusammenpack-Code niedergelegt worden. Dieser Zusammenpack-Code ordnet jedem Stoff der Klassen 3, 6.1 und 8 einer mit einem Großbuchstaben dargestellten Packkategorie zu. Er legt damit fest, mit welchen anderen Stoffen - nämlich mit denen gleicher Klasse und Pack-Kategorie der Stoff zusammengepackt werden kann. Eine Ausnahme bildet die Packkategorie X. Stoffe, die dieser Kategorie zugeordnet sind, dürfen nicht mit anderen Stoffen zusammengepackt werden. Stoffe, die nicht der GGVS unterliegen, dürfen grundsätzlich nicht mit Gefahrgütern zusammengepackt werden. Die in dieser Datei enthaltenen Pack-Kategorien beziehen sich nur auf den Landverkehr.” /CSD/

Gefahrgutverordnung Eisenbahn bzw. Straße = GGVE/GGVS

“Diese Verordnung gilt für den Zuständigkeitsbereich der Deutschen Bahn bzw. für das gesamte öffentliche Straßennetz der Bundesrepublik Deutschland. Die Klassen und Ziffer der Stoffaufzählung werden angegeben sowie bei Bedarf wird auch die Verpackungsgruppe angegeben.

Beispiel: GGVE/GGVS 6.1/41a = Bromzyan”/CSD/

Für See- und Binnenschiffahrt als auch für den Luftverkehr gelten ähnliche Verordnungen (z.B. Gefahrgutverordnung-See, GGV-See). Die Gefahrgut-klassen sind jedoch für alle Verkehrsträger gleich. Es bedeuten:

“1: *Explosivstoffe*
2: *Gase*
3: *Entzündbare flüssige Stoffe*
4.1: *Entzündbare feste Stoffe*
4.2: *Selbstentzündliche Stoffe*
4.3: *Stoffe, die in Berührung mit Wasser entzündbare Gase entwickeln.*

5.1: *Entzündend (oxidierend) wirkende Stoffe*
5.2: *Organische Peroxide*
6.1: *Giftige Stoffe*
6.2: *Ekelerregende oder ansteckungsgefährliche Stoffe*
7: *Radioaktive Stoffe*
8: *Ätzende Stoffe*
9: *Verschiedene Stoffe*

Die Stoffe der "Nur Klassen" 1, 2, 4.2, 4.3, 5.2, 6.2 und 7 dürfen nur befördert werden, wenn sie den jeweiligen besonderen Bestimmungen entsprechen. Sofern eine dieser Klassen ohne ergänzende Ziffer oder UN-Nummer angegeben ist, ist der Versand nur unter speziellen Bedingungen oder aufgrund von zwischenstaatlichen Vereinbarungen möglich, die hier nicht aufgeführt sind." /CSD/

7.3.3 Lagerklasse

"Jedem Artikel ist, abhängig von seinen Gefahrenmerkmalen, eine Lagerklasse (LGK) zugeordnet. Die Definition der Lagerklassen entspricht dem "Konzept zur Zusammenlagerung von Chemikalien" des VCI. Grundlage dieses Konzeptes sind Gesetze, Vorschriften und Technische Regeln der Bundesrepublik Deutschland. Es bedeuten:
2A: *Verdichtete, verflüssigte oder unter Druck gelöste Gase.*
2B: *Druckgaspackungen (Aerosoldosen)*
3A: *Entzündliche flüssige Stoffe. (Flammpunkt bis 55 Grad C).*
3B: *Brennbare Flüssigkeiten (VbF AIII).*
4.1A: *Entzündbare feste Stoffe. (2. SprengV: Lagergruppe I-III).*
4.1B: *Entzündbare feste Stoffe. (EG-Methode A 10).*
4.2: *Selbstentzündliche Stoffe.*
4.3: *Stoffe, die in Berührung mit Wasser entzündliche Gase bilden.*
5.1A: *Entzündend wirkende Stoffe. (TRGS 515 Gruppe 1).*
5.1B: *Entzündend wirkende Stoffe. (TRGS 515 Gruppe 2+3).*
5.2: *Organische Peroxide.*
6.1: *Giftige Stoffe.*
7: *Radioaktive Stoffe.*
8: *Ätzende Stoffe.*
10: *Brennbare Flüssigkeiten soweit nicht LGK 3A bzw. LGK 3B.*
11: *Brennbare Feststoffe.*
12: *Nicht brandgefährliche Flüssigkeiten in nicht brandgefährlicher Verpackung.*
13: *Nicht brandgefährliche Feststoffe in nicht brandgefährlicher Verpackung.*

Artikel einer Lagerklasse dürfen in der Regel in einem Lagerabschnitt gelagert werden. Die Zusammenlagerung von Artikeln verschiedener Lagerklassen wird ausführlich durch eine Tabelle Separat- oder Zusammenlagerung im VCI-Konzept beschrieben. Flüssige und feste Stoffe, Zubereitungen und Erzeugnisse, die nicht die Kriterien der LGK 1 - 8 erfüllen, werden in dieser Datei mit LGK 10 - 13 gekennzeichnet. Auf eine weitere Differenzierung zwischen den Lagerklassen 10, 11, 12 und 13 wird in dieser Datei verzichtet da die Lagerklassen stoffbezogen angegeben werden. Die Brennbarkeit der Einheit Stoff/Verpackung kann deshalb nicht beurteilt werden. Gesetzliche Zusammenlagerungsbeschränkungen innerhalb der Lagerklassen 10 - 13 gibt es nicht. Bei der Zusammenlagerung von Artikeln der LGK 10 - 13 mit anderen Lagerklassen muss bei Anwendung der Tabelle Separat- oder Zusammenlagerung die Brandgefährlichkeit von Stoff und Verpackung berücksichtigt werden." /CSD/

7.3.4 Verordnung für brennbare Flüssigkeiten (VfB)

"Nach dieser Verordnung werden Lösungsmittel in die folgenden Gefahrklassen eingeteilt:

A I: *Mit Wasser nicht oder nur teilweise mischbare Flüssigkeiten mit einem Flammpunkt unter 21 Grad C.*

A II: *Mit Wasser nicht oder nur teilweise mischbare Flüssigkeiten mit einem Flammpunkt zwischen 21 und 55 Grad C.*

A III: *Mit Wasser nicht oder nur teilweise mischbare Flüssigkeiten mit einem Flammpunkt zwischen 55 und 100 Grad C.*

B: *Für mit Wasser bei 15 Grad C in jedem Verhältnis mischbare Flüssigkeiten mit einem Flammpunkt unter 21 Grad C.*

Bedauerlicherweise sind diese Definitionen nicht mit der Abgrenzung der Gefahrensymbole F (leicht entzündlich) und F+ (hochentzündlich) identisch. Eine Kennzeichnungspflicht nach der VbF besteht in erster Linie für Anlagen zur Lagerung, Abfüllung oder Beförderung von brennbaren Flüssigkeiten. In chemischen Laboratorien ist diese Kennzeichnung daher im allgemeinen nicht notwendig." /CSD/

7.3.5 Weitere, oft verwendete Kennzeichnungen

“UN-Nummer

Das Experten-Komitee der Vereinten Nationen (UN) gibt Empfehlungen für alle Verkehrsträger heraus, betreffend die Einstufungen von gefährlichen Gütern zu Transportzwecken. Sie werden fortlaufend nummeriert. Unterschiedliche UN-Nummern bei dem gleichen Artikel können sich aus terminlichen oder technischen Gründen ergeben. Im Luftversand kann u.U. anstelle der UN-Nr. eine ID-Nr. Verwendung finden.

Beispiel: UN 1889 = Bromzyan

EG-Nummer

Diese Nummer wird von der EG-Kommission zur Einstufung, Verpackung und Kennzeichnung gefährlicher Stoffe vergeben. Bei Zubereitungen und Mischungen wird jeweils die Zuordnung nach der hauptsächlichen Komponente getroffen. Letzteres gilt auch für die Zuordnung der CAS-Nummer.

Beispiel: EG-Nr. 616-011-0-4 = N,N-Dimethylacetamid

IATA/CAO

IATA = International Air Transport Association
ICAO = International Civil Aviation Organization

Da die "Technical Instruction" der ICAO (Internationale Zivil-Luftfahrt Organisation der UN) noch nicht in die Gesetzgebung der Bundesrepublik übernommen wurde, basieren die Angaben in dieser Datei auf der 32. Ausgabe der "Dangerous Goods Regulation" der IATA (Vereinigung der Luftverkehrs-Gesellschaften). Angegeben werden Klasse und UN-Nummer bzw. ID-Nummer. Sondervorschriften von Staaten oder Fluggesellschaften sind nicht berücksichtigt.

Beispiel: IATA/CAO 6.1 UN 1889 = Bromcyan

IMDG

= International Maritime Code for Dangerous Goods

Der IMDG-Code ist eine Ausarbeitung der IMO (International Maritime Organization der UN). In der Bundesrepublik Deutschland ist der IMDG-Code Bestandteil der GGV-See. Angegeben werden Klasse (siehe GGVE/GGVS), Verpackungsgruppe und UN-Nummer. Die Angaben entsprechen dem 25. Amendment, soweit nicht abweichende oder weitergehende Vorschriften der GGV-See bestehen.

Beispiel: IMDG 6.1/I UN 1889 = Bromcyan

ID-Nummer
Wenn keine UN-Nummer vorliegt, jedoch eine Kennzeichnung erforderlich ist, vergibt die IATA eine Identifizierungs-Nummer.

Beispiel: ID 8004 = Reagenzien-Sätze" /CSD/

7.4 Zwei öffentlich geförderte Programmbeispiele

In diesem Abschnitt werden zwei Programme vorgestellt, die von der öffentlichen Hand finanziert, gefördert und unterhalten wurden und werden. In diesen Programmen werden Informationen zu gefährlichen Stoffen angeboten. Für die EDV-unterstützte Erstellung von Sicherheitsdatenblättern, Betriebsanweisungen usw. muss man jedoch auf kommerzielle Programme zurück greifen.

7.4.1 Gefahrstoffdatenbank der Länder (GDL)

"Aufbauend auf der Grundlage des Chemikaliengesetzes und der Arbeitsstoffverordnung sowie später der Gefahrstoffverordnung erarbeiteten die Länder Baden-Württemberg, Rheinland-Pfalz und Hessen bereits 1982 eine gemeinsame Gefahrstoffdatenstrukturrichtlinie, die als Grundlage für einen kostenlosen Datenaustausch untereinander diente. Aus diesen Aktivitäten heraus entwickelte sich ein Länderarbeitskreis, der sich die arbeitsteilige Erfassung und Pflege von Stoff- und Zubereitungsdaten zum Ziel gesetzt hatte. Mit dem einstimmig verabschiedeten Beschluss der 62. Arbeits- und Sozialministerkonferenz wurden 1986 alle im Länderausschuss für Arbeitsschutz und Sicherheitstechnik (LASI) vertretenen Bundesländer in die Fachgruppe \`Gefahrstoffdatenbank der Länder´ (GDL) eingebunden. ...
Mit dem LASI-Beschluß vom 23/24. 01. 89 wurde die Fachgruppe "GDL" dem Unterausschuss II "Gefahrstoffe" des LASI zugeordnet. Dieser Ausschuss fungiert u.a. als Lenkungsgremium für die Gefahrstoffdatenbank der Länder innerhalb des LASI.
Die Fachgruppe "GDL" hat im wesentlichen folgende Aufgaben:

⇒Erarbeitung und Fortschreibung des benötigten Datenaustauschformates

⇒arbeitsteilige Erhebung, Erfassung und Pflege von Stoff- und Zubereitungsdaten

⇒kostenloser Austausch von nicht vertraulichen Stoff- und Zubereitungsdaten." /HMW/

"Als Koordinierungsstelle sammelt und integriert die Bundesanstalt für Arbeitsschutz alle von den einzelnen Kooperationsmitgliedern erarbeiteten Daten. Der jeweils aktualisierte Gesamtdatenbestand wird mit Ausgabe-programmen in regelmäßigen Abständen (z.Z. halbjährlich) kostenlos an alle Fachgruppenmitglieder und Kooperationspartner verteilt. ...

Wesentlich in dieser Kooperation ist nicht nur der kostenlose Austausch der Stoffdaten, sondern auch die Ausschließung der kommerziellen Nutzung der Daten. ...
In der Kooperation arbeiten Partner mit unterschiedlichen DV-Umgebungen zusammen (IGS <–> UNIX, GDL <–> PC, HVBG <–> Großrechnerlösung). Um den vollständigen Datenaustausch zwischen diesen unterschiedlichen DV-Systemen sicherzustellen, wurde eine Standard-Stoffdaten-Austausch-Schnittstelle entwickelt. Die Schnittstelle ist systemunabhängig und kann beliebige Stoffe, Merkmale mit Randbedingungen (Spezifikationen), sowie Managementinformationen übertragen. Der Datenaustausch findet auf der Basis dieser Schnittstelle mit abgestimmten Referenzlisten statt. ...
Die Gefahrstoffdatenbank enthält z.Z. ca. 16.000 Stoffdatensätze, davon ca. 6.000 Produkte, mit bis zu 180 Einzelmerkmalen pro Stoff." /HMW/
"Der Inhalt der Datenbank wird aus eigenen Daten, Informationen aus anderen Datenbanken, den Ergebnissen aus der Eigenschaftsermittlung durch beauftragte wissentliche Institute und Eigenerhebungen aus Gesetzestexten und Fachliteratur zusammengestellt. Da die unterschiedlichen Datenquellen keine einheitlichen Stoffnamen verwenden, erfolgt die Stoffidentifikation in der GDL über Identifikationsmerkmale." /Wun/ Dazu existiert in der GDL eine Identifikationsdatei.
"In der Identifikationsdatei wird einem bestimmten Stoff, einer bestimmten Zubereitung oder einer Stoffgruppe eindeutig eine Systemnummer, die sogenannte Fachgruppen-Nummer (FG-NR) zugeordnet. ...
Über die Identifikationsdaten hinausgehend sind in der Gefahrstoffdatenbank Stoffaktendaten und die dazugehörigen Managementinformationen vorhanden. Die GDL-Daten sind in folgende Themenbereiche gegliedert:

⇒Identifikation

⇒Physikalisch-chemische Daten

⇒Toxikologie

⇒Ökotoxikologie

⇒Umgang/Verwendung

⇒Einstufung/Kennzeichnung

⇒Gesetzliche Regelung/Vorschriften

⇒Analyseverfahren" /HMW/

"Als wichtigste Quelle für Informationen zu Zubereitungen ist das Sicherheitsdatenblatt gedacht. Aus den Sicherheitsdatenblättern der Hersteller werden die Sicherheitskenndaten für Zubereitungen übernommen. Dies sind die für den

Umgang wesentlichen physikalischen, sicherheitstechnischen, toxikologischen und ökotoxikologischen Daten sowie Empfehlungen für einen sicheren Umgang. Aufgrund des Chemikaliengesetzes (ChemGes) sind die Hersteller von neuen Stoffen verpflichtet, diese spätestens 45 Tage vor Inverkehrbringen bei der Anmeldestelle nach ChemGes (BAU) anzumelden. ...
Wichtig für die vollzugsorientierten Behörden und sonstige Stellen sind Daten aus dem Bereich Umgang/Verwendung, worin, resultierend aus den Gefährlichkeitsmerkmalen des Stoffes, Verhaltensregeln für den Umgang und Maßnahmen für den Störfall erarbeitet wurden. ...
Ebenfalls von Bedeutung für die Überwachungsbehörden sind Merkmale aus den Themenbereichen Einstufung/Kennzeichnung und Vorschriften/ Grenzwerte (TRGS 900, TRGS 903, TRGS 905, TA Luft, Stoffliste gem. §4a GefahrstoffV, GGVS, Störf, Ausländische Grenzwerte)." /HMW/

7.4.2 Informations- und Kommunikationssystem für gefährliche und umweltrelevante Stoffe (IGS)

"Unter dem Eindruck des Sandoz-Störfalls begann das Land Nordrhein-Westfalen 1988 unter Federführung des Ministeriums für Umwelt, Raumordnung und Landwirtschaft (MURL) mit der Entwicklung eines landesweiten Stoff-Informationssystems. Folgende Vorgaben sollte das System realisieren:
⇒Bündelung der Informationsfülle,
⇒allgemeinverständliche Darstellung der fachwissenschaftlichen Daten,
⇒schnellste Verfügbarkeit der Daten vor Ort - besonders in Hinblick auf die Gefahrenabwehr/-bekämpfung,
⇒einheitliches Informationssystem für alle Behörden, um einen reibungs-losen Informationsaustausch zu gewährleisten.
Das Ziel des Informationssystems ist es, den für Gefahrenabwehr und Umweltschutz zuständigen Behörden unmittelbar an ihre speziellen Aufgaben angepasste, verlässliche Stoffinformationen bereitzustellen. ...
Aus dem Konzept für das landesweite Informationssystem entstand das \`**I**nformations- und Kommunikationssystem **G**efährliche/umweltrelevante **S**toffe´, kurz IGS genannt.
Der Kern der IGS ist eine zentrale Datenbank im FIZ, die in ständiger Fortschreibung die relevanten Stoffinformationen umfassend enthält. Die zentrale Datenbank stellt Informationen zu allen relevanten Themen bereit:
⇒Stoffidentifikation

⇒physikalisch-chemische Eigenschaften

⇒Gefahrenpotentiale

⇒Toxikologie

⇒Ökotoxikologie

⇒Handhabung

⇒Einsatzmaßnahmen

⇒Erste Hilfe

⇒Analytik, Umweltverhalten

⇒gesetzliche Regelungen

⇒Entsorgung

Der Grunddatenbestand ist durch Einbeziehung von mehr als 20 Datenquellen aufgebaut. Insgesamt umfasst der Datenbestand derzeit 11.000 Stoffe, die unter 35.000 Synonymen und Produktnamen abrufbar sind. Pro Stoff enthält die Datenbank bis zu 200 verschiedene Einzelangaben. Weitere 3.000 Stoffe sind ausschließlich aufgrund ihrer Nennung in Rechtsvorschriften berücksichtigt.
Den einzelnen Nutzergruppen - z.B. Feuerwehr, Polizei, Gewerbeaufsicht - wird der Datenbestand vor Ort als IGS-Anwendung zur Verfügung gestellt. Eine IGS-Anwendung besteht sowohl aus dem Datenmaterial als auch aus der Anwendungssoftware und ist unter anderem auf einem PC/Laptop lauffähig." /LNW/
Das IGS-System wurde an die jeweiligen Bedürfnisse der einzelnen Anwendergruppen angepasst und existiert daher in verschiedenen Ausführungen:
⇒IGS-fire
Diese Version soll Polizei und Feuerwehr unterstützen bei der Schadensbegrenzung und Bekämpfung von Unfällen, Unglücken, Bränden o.ä. bei denen gefährlicher Stoffe beteiligt sind. Dazu stellt das System die Kapitel `Gefahren´ und `Maßnahmen´ zur Verfügung. Reicht dies nicht aus, werden im Kapitel `Stoffdaten´ dem Experten vor Ort stoffspezifische Daten zur Bewertung des Stoffes und der Situation geboten. Der Anwender kann eigene Erfahrungen und Informationen im Kpt. `Maßnahmen´ eingeben. Dazu gibt es die Menüpunkte `Standortinfo´ und `Einsatzdokumentation´. Sollten keine detaillierten Stoffinformationen vorliegen, kann der Anwender auch über den `Gefahrenzettel´ suchen. Er erhält dann stoffgruppenbezogene Hinweise.
⇒IGS-water
Hier soll den Behörden, die für den Gewässerschutz zuständig sind, eine Arbeitsgrundlage gegeben werden. Das Verhalten von Stoffen in Wasser als auch Ökotoxikologie und Ökologie sind die Schwerpunkte des Programms. Ansonsten ist das Programm inhaltlich vergleichbar mit IGS-check.

⇒IGS-check
Diese Version ist insbesondere zur Erleichterung der Tätigkeit der Gewerbeaufsichtsbeamten entwickelt worden. Dateninhalt und Präsentationslogik sind auf die Anforderungen des Arbeits- und Immissionsschutzes abgestimmt. Folgende Gesetze und Verordnungen werden berücksichtigt und vom Programm (als Argumentationsbasis) zur Verfügung gestellt:

◊ Gefahrstoffverordnung
◊ Störfallverordnung
◊ TRGS 900 und TRGS 500
◊ Gefahrgutverordnungen für Straße, Schiene, See, Binnenschifffahrt und andere diesbezügliche Vorschriften
◊ Katalog wassergefährdender Stoffe

IGS-check bietet weiterhin Informationen u.a.

◊ zum Personenschutz und zu Gesundheitsgefahren,
◊ zu Gefahren und Maßnahmen bei Brand und Explosionen,
◊ zu den physikalisch-chemischen Eigenschaften,
◊ zu Messverfahren,
◊ zur Lagerung und zum Transport,
◊ zur Umweltverträglichkeit und Entsorgung.

Auch Vorlagen zur Erstellung von Betriebsanweisungen nach TRGS 555 können mit dieser Programmversion erstellt werden.

⇒TRANSEC
TRANSEC unterstützt die Kontrolle von Gefahrguttransporten vor Ort. Die Gefahrgutverordnung Straße sowie die einschlägigen europäischen Regelungen sind stoff- und transportspezifisch aufbereitet worden. Es stellt eine Checkliste zur Verfügung, die eine Gefahrgutkontrolle Punkt für Punkt ermöglicht. Je nach Ergebnis der Kontrolle druckt das System automatisch eine Kontrollbescheinigung, ein Bußgeldbescheid oder ein Transportverbotsbescheid aus.

⇒IGS-Hochschule
Speziell für die Hochschulen wurde IGS-Hochschule entwickelt. Als Basis diente IGS-check als Recherchemodul. Die Verwaltung der in der Hochschule vorhandenen Gefahrstoffe als auch die Dokumentation der Hoch-schulinternen Entsorgungsdaten soll erleichtert werden. Das System bietet auch die Möglichkeit bisher in IGS-check nicht dokumentierte Stoffdaten zu erfassen und anderen Anwendern zugänglich zu machen.

7.5 Anforderungen an ein Gefahrstoffprogramm
Wenn ein solches Programm beschafft werden soll, ist es notwendig auf manche Dinge zu achten, die man vorher entweder als selbstverständlich und gegeben oder als unwichtig oder unnötig erachtet hat.
Manches Programm benötigt bestimmte Hardware und/oder Software (Betriebssystem, Benutzeroberfläche usw.) Oft werden bestimmte EDV-Kenntnisse des Anwenders vom Entwickler und später vom Vertreiber solcher Programme vorausgesetzt. Bei den Planungen der Kosten der Programmbeschaffung wird gern vergessen, dass häufig Kosten für Schulung, Programmpflege, Hotline-Service, technische Unterstützung bei Installation und Einführung anfallen. Dazu kommt, dass gerne der Erstarbeitsaufwand vollkommen falsch eingeschätzt wird, in der Regel viel zu niedrig angesetzt ist. Man sollte sich auch mit den allgemeingültigen Regeln zu Softwareergonomie und Datenschutz/-sicherheit vertraut machen. So werden jetzt noch in manchen Programmen elementare software-ergonomische Regeln nicht beachtet bzw. nicht angewendet.

7.5.1 Allgemeine Anforderungen
Nach DIN sollte ein Programm (ganz allgemein gültig) folgende Grundsätze erfüllen. Es sollte

1. aufgabenangemessen,
2. selbstbeschreibungsfähig,
3. steuerbar,
4. erwartungskonform und
5. fehlerrobust sein.

Aufgabenangemessen bedeutet, dass der Anwender bei der Erfüllung seiner Aufgaben vom Programm unterstützt wird, ohne zusätzlich durch Eigenschaften des Programms belastet zu werden. D.h. also, dass solch ein Programm die Arbeit erleichtern und nicht erschweren soll.
Will man z.B. neue Stoffdaten eingeben, sollten übersichtliche und geordnete Eingabemasken da sein. Der Datenblattaufbau sollte immer gleich sein. Sinnvolle Vorgaben, die einfach überschrieben werden können, unterstützen die Eingabe zusätzlich.
Wenn (z.B. Stoff-) Daten ausgegeben werden, sollten sie formatiert sein, dass der Anwender sich leicht zurechtfindet. Alle wichtigen Daten (des Stoffes) sollten leicht aufnehmbar sein.

Selbstbeschreibungsfähig ist ein Programm dann, wenn es dem Anwender direkte Informationen über seinen Umfang, seinen Aufbau, seine Aufgaben und seine Steuerbarkeit gibt. Das bedeutet für ein Gefahrstoffprogramm: man soll

sehen, was das Programm alles leistet bzw. was es für Module (Gefahrstoffkataster, Sicherheitsdatenblatt, Betriebsanweisung usw.) anbietet, wo man sich befindet (Sicherheitsdatenblatt erstellen, neue Gefahrstoffdaten eingeben, Betriebsanweisung ausdrucken ...), wo man wie hingelangt (z.B. von Gefahrstoffeingabe zu Sicherheitsdatenblatt erstellen). Die Dialogschritte haben unmittelbar verständlich zu sein.
Ein Hilfemodul soll dem Anwender auf Verlangen Informationen zur Handhabung, zu bestimmten Feldern oder Meldungen in einer ihm verständlichen Ausdrucksweise geben. Für die Dateneingabe eines noch nicht erfassten Stoffes in einem Gefahrstoffdatenblatt bedeutet dies, dass entweder die Titel der Eingabefelder so gewählt sind, dass man weiß, was man einzugeben hat oder falls dies nicht möglich ist, für die Felder ein Erklärung angeboten wird, welche die notwendigen Informationen zur Eingabe beinhaltet.

Ein Programm wird als *steuerbar* bezeichnet, wenn es dem Anwender ermöglicht, ohne starre Menüabläufe von einem Teil des Programms zu einem anderen zu gelangen. Beispielsweise sollte man von Eingabe von Gefahrstoffdaten direkt zu Ausdrucken oder Erstellen eines Sicherheitsdatenblattes wechseln können, ohne zum Ausgangsmenü zurückzukehren. Es ist auch wichtig, dass man einen Arbeitsschritt unterbrechen oder gar abbrechen kann. Der letzte Arbeitsschritt sollte widerrufbar sein. Verarbeitungsprozesse, die eine größere Tragweite haben, sollten erst nach einer Bestätigung ausgelöst werden. Es ist natürlich irgendwo nervend, wenn man vom Programm irgendwas besonderes verlangt, dies dauernd noch mal extra zu bestätigen. Spätestens aber, wenn man ein Gefahrstoffdatenblatt aus Versehen gelöscht hat und dieses wieder frisch eingeben muss, lernt man die beiden letztgenannten Forderungen zu schätzen.
Eine Forderung ist (leider) immer noch bei vielen Programmen nicht realisiert: Bei Unterbrechungen und Störungen durch einen Systemausfall sollte der Anwender seine Arbeit beim letztdurchgeführten Dialogschritt wieder aufnehmen können. Eine Realisierung dieser Forderung bedeutet, dass nach jedem Arbeitsschritt gesichert werden muss. Darunter leidet natürlich die Schnelligkeit des Programms.

Ein Programm verhält sich *erwartungskonform*, wenn

⇒das Programm sich so verhält, wie im Handbuch beschrieben ist,

⇒das Dialogverhalten und die Dialogführung einheitlich ist,

⇒(gleiche) Aktionen des Anwenders sofort zu (gleichen) Reaktionen des Programms führen und

⇒Abweichungen von den ersten drei Punkten erklärt werden.

Diese Erwartungskonformität ist der Hauptgrund, warum ein Gefahrstoffdatenblatt, ein Sicherheitsdatenblatt oder eine Betriebsanweisung immer gleich aufgebaut sein sollen - nicht nur im Programm!

Die Eigenschaft `*fehlerrobust*´ ist mittlerweile Standard. Man bringt durch falsche Eingaben fast keine Programme mehr zum Absturz. Auch die Informationen über Art und Ort des Fehlers sind in der Regel ausreichend. Nur die Hinweise zur Fehlerbehebung sind in manchen Programmen etwas dürftig geraten.

7.5.2 Gefahrstoffprogrammspezifische Anforderungen

Die bisher beschriebenen Anforderungen gelten auch für andere Programme wie z.B. die im nächsten Kapitel beschriebenen Unfalldaten-erfassungs- und -verarbeitungsprogramme. Es folgen jetzt einige Anforderungen, die speziell für Gefahrstoffprogramme gelten.

Im Datenbankteil sollten schon möglichst Daten vieler Stoffe als fertige Datensätze zur Verfügung stehen. Die Datensätze sollten alle Daten enthalten, die für das Erstellen eines Sicherheitsdatenblattes, einer Betriebsanweisung o.ä. notwendig sind. Dazu ist es leider oft notwendig, dass die Datensätze viele Unterpunkte enthalten, worunter die Übersichtlichkeit im allgemeinen etwas leidet. Eine bedeutende Arbeitserleichterung ist die Möglichkeit, externe Datensätze einzulesen. Muss man die Daten selbst eingeben, ist es von Vorteil, einen schon ausgefüllten Datensatz benutzen zu können. In so einem Fall sollte eine Sicherung da sein, dass man den ursprünglichen Datensatz nicht löscht, indem man unter dem alten Namen abspeichert. Wichtig ist, wie schon im vorhergehenden Abschnitt erklärt, dass die Datenblätter/-sätze alle gleich aufgebaut sind. Wenn man in der Datenbank etwas sucht, sollte es möglich sein, alle Unterpunkte als Suchkriterium zu verwenden. Ebenso sollten die Daten nach allen Unterpunkten sortierbar sein.

Erstellt man ein Sicherheitsdatenblatt, eine Betriebsanweisung, ein Unfall-merkblatt o.ä. ist es vorteilhaft, wenn schon vorformatierte Masken zur Verfügung stehen. Erstellt man diese für einen Stoff, der schon in der Datenbank registriert ist, sollten entsprechende stoffabhängige Angaben automatisch eingefügt werden. Fast schon eine Selbstverständlichkeit ist mittlerweile, dass R- und S-Sätze sowie Gefahren-, Verbots- und Gebots-symbole zur Verfügung stehen.

Folgende Anforderungen sollte eine Gefahrstoffdatenbank also erfüllen:

⇒Möglichst viele Stoffe als Datensätze

⇒Immer gleicher Datenblattaufbau

⇒Datensätze mit möglichst vielen Unterpunkten

⇒Externe Datensätze sind einlesbar

⇒Suchmöglichkeit nach allen Unterpunkten

⇒Gute Ergänzungsmöglichkeit

⇒Automatische Sicherung

⇒Sicherung gegen versehentliches Überschreiben
⇒Betriebsanweisungen sind erstellbar, am besten vorformatiert
⇒Sicherheitsdatenblatt ist erstellbar, am besten vorformatiert
⇒Unfallmerkblatt ist erstellbar, am besten vorformatiert
⇒Gefahrstoffkataster ist erstellbar
⇒Daten, die stoffspezifisch sind, werden automatisch eingetragen
⇒S- und R-Sätze stehen zur Verfügung
⇒Gefahren-, Verbots- und Gebotssymbole stehen zur Verfügung

8 Unfalldatenerfassungs- und -bearbeitungsprogramme

Unfalldatenerfassungs- und -bearbeitungsprogramme werden in großen und mittelgroßen Betrieben gerne als Unterstützung der "Sicherheitsarbeit" und auch zur möglichen Arbeitserleichterung und -rationalisierung verwendet.
Weshalb?
Die schönen Anfangserfolge der betrieblichen Sicherheitsarbeit stagnierten in der Regel. Die alleinige konsequente Anwendung der Grundlagen der Sicherheitstechnik reichte nicht mehr aus, um eine weitere Verringerung des Unfallgeschehens zu erreichen. Um das Ziel "Unfallhäufigkeitsreduzierung" weiter verfolgen zu können, mussten andere Methoden und Hilfsmittel zum Einsatz kommen.
Dazu kam/kommt das Problem, dass der Aufgabenbereich einer FaSi häufig immer mehr ausgedehnt wurde/wird. Die üblichen Routineaufgaben einer FaSi, wie die Erstellung betriebsinterner und berufsgenossenschaftlicher Unfallmeldungen, der sich daraus ergebenden Statistiken und Kostenrechnungen sowie die Koordinierung von Schulungen und die Verwaltung der persönlichen Schutzausrüstung war und ist weiterhin zeitraubend. Daher war es notwendig, im quantitativen Bereich Mittel zur Arbeitseffektivvisierung zu finden.
Eines dieser Mittel zur Verbesserung der Quantität als auch der Qualität der Arbeit einer FaSi ist nun der Gebrauch von Computern unter Verwendung entsprechender "Arbeitsschutz-Software". Seit Mitte der achtziger Jahre wurde Software zur Unfalldatenaufnahme, -bearbeitung und statistischen Auswertung im größeren Stil entwickelt. Hierbei war es u.a. notwendig, die Anforderungen der Berufsgenossenschaften an eine Unfallanzeige zu erfüllen, um die doppelte Aufnahme der Unfalldaten zu vermeiden. Auch andere Regelungen waren zu berücksichtigen, die entweder von den Berufsgenossenschaften oder dem Gesetzgeber geschaffen wurden.
Da in der Regel PCs benutzt worden, fiel - aufgrund des mangelnden Arbeitsspeichers - der u.E. sehr wichtige statistische Teil bei den meisten Programmen etwas dürftig aus. Dies ist mittlerweile bedeutend besser.

8.1 Exkurs: Arbeitsschutzrecht

Das deutsche Arbeitsschutzrecht ist historisch gewachsen. Die Grundlagen liegen in der Gesetzgebung des späten 19. Jahrhundert. Einige der heute noch geltenden Bestimmungen stammen aus diesem Zeitraum. So sind z.B. die Anfänge der Reichsversicherungsordnung (RVO, ist im Sozialgesetzbuch aufgegangen) und der Gewerbeordnung in dieser Zeit geschaffen worden. Aus dieser Zeit stammt der auch heute noch geltende Dualismus im Arbeits-

schutzrecht (dies hat sich durch das europäische Recht auf dem Papier geändert, aber u.E. noch keine wesentlichen praktischen Auswirkungen gezeigt), der den Staat (als Gesetzgeber) auf der einen Seite und die Berufsgenossenschaften (als Versicherungsträger) auf der anderen Seite zu nahezu gleichberechtigten Handlungspartnern auf dem Feld des Arbeitsschutzes macht. Der Staat übt seinen Einfluss durch Gesetze und Verordnungen aus, die Berufsgenossenschaften durch Unfallverhütungsvorschriften und -anweisungen. Ergänzt werden diese durch Normen (z.B. von DIN, VDE usw.), Sicherheitsregeln, technische Regeln und Tarif- und Betriebsvereinbarungen. Überwacht werden diese Bestimmungen durch staatliche Stellen und/oder durch die Unfallversicherungsträger und andere private Institutionen (z.B. TÜV, Sachverständige).

8.1.1 (staatliche) Gesetze und Verordnungen

In den vom Staat verfügten Regelungen (durch Gesetze/Verordnungen) werden insbesondere die Mindestanforderungen zum Arbeitsschutz festgelegt. Das Arbeitszeitrecht, der Schutz besonderer Arbeitnehmergruppen (z.B. Schwerbehinderte, Jugendliche, Schwangere), die allgemeine Sicherheit in den Betrieben (inklusive Hygiene), der vorgreifende technische Arbeitsschutz (z.B. Umgang mit Gefahrstoffen, Handhabung von Arbeitsmitteln) sind Schwerpunkte der gesetzlichen Regelungen. Die wichtigsten staatlichen Regelungen sind:

⇒Arbeitsschutzgesetz
⇒Chemikaliengesetz
⇒Gesetz über technische Arbeitsmittel (Gerätesicherheitsgesetz)
⇒Jugendarbeitsschutzgesetz
⇒Mutterschutzgesetz
⇒Schwerbehindertengesetz
⇒Bürgerliches Gesetzbuch
⇒Sozialgesetzbuch
⇒Gewerbeordnung
⇒Gefahrstoffverordnung
⇒Arbeitsstättenverordnung
⇒Arbeitsstättenrichtlinien

Das Arbeitsschutzgesetz wurde im Juni 1996 verabschiedet. Auf dessen Basis worden und worden Verordnungen erlassen, die das europäische Arbeitsschutzrecht in der Regel nahezu eins zu eins übernehmen (z.B. die in Kpt. 5 besprochene Bildschirmverordnung).
Das Chemikaliengesetz und die Gefahrstoffverordnung regeln den Umgang mit Gefahrstoffen (vgl. Kpt. Sieben).

Im Gerätesicherheitsgesetz werden die Mindestanforderungen festgelegt, welche die Sicherheit von Geräten betreffen, die in Deutschland in Verkehr gebracht werden sollen.
Die nächsten drei erwähnten Gesetze wurden zum Schutz von besonders gefährdeten Arbeitnehmergruppen erlassen, um auch diesen Gruppen ein möglichst gefährdungsfreies Arbeiten zu ermöglichen.
Das Bürgerliche Gesetzbuch (BGB) enthält wichtige Regelungen zur Fürsorgepflicht des Arbeitgebers im Rahmen des Beschäftigungsverhältnisses.
Die Auswirkungen des siebten Buches des Sozialgesetzbuches haben im Rahmen dieses Kapitels eine wichtige Bedeutung. Dieses siebte Buch ist die Grundlage der gesetzlichen Unfallversicherung. Sie regelt die Aufgaben der Berufsgenossenschaften z.B. Entschädigung von Arbeitsunfällen, Rehabilitierung Betroffener nach Arbeitsunfällen und Berufskrankheiten sowie die Prävention vor Arbeitsunfällen und Berufskrankheiten. So müssen Arbeitsunfälle, die zu einer Ausfallzeit des Betroffenen von drei oder mehr Tagen führen dem zuständigen Versicherungsträger gemeldet werden. Die Versicherungsträger sind ermächtigt und verpflichtet Unfallverhütungsvorschriften zu erlassen.

8.1.2 Unfallverhütungsvorschriften

Die Versicherungsträger (d.h. in der freien Wirtschaft die Berufsgenossenschaften) erlassen Unfallverhütungsvorschriften (UVVen) über:

⇒"Einrichtungen, Anordnungen und Maßnahmen, die die Unternehmer zur Verhütung von Arbeitsunfällen und Berufskrankheiten zu treffen haben, einschließlich der Form der Übertragung dieser Aufgaben auf andere Personen,

⇒das Verhalten, das die Versicherten zur Verhütung von Arbeitsunfällen und Berufskrankheiten zu beachten haben,

⇒ärztliche Untersuchungen von Versicherten, die vor der Beschäftigung mit Arbeiten durchzuführen sind, deren Verrichtung mit außergewöhnlichen Unfall- oder Gesundheitsgefahren für sie oder Dritte verbunden ist,

⇒die Maßnahmen, die der Unternehmer zur Erfüllung der sich aus dem Arbeitssicherheitsgesetz (Anm. d. Autoren: nun Arbeitsschutzgesetz) ergebenden Pflichten zu treffen hat." /Gra, S.52/

"Der konzeptionelle Aufbau der Unfallverhütungsvorschriften ist darauf abgestellt, dass einerseits allgemeine, für jedes Unternehmen geltende Bestimmungen aufgestellt werden (Basis-Unfallverhütungsvorschriften), darüber hinaus aber auch spezielle tätigkeits- wie auch objektbezogene Unfallverhütungsvorschriften bestehen." /Gra, S.52/
Die Titel der Basis-Unfallverhütungsvorschriften sind genügend aussagekräftig, um mit einer Aufzählung auszukommen:

⇒UVV "Allgemeine Vorschriften"

⇒UVV "Erste Hilfe"

⇒UVV "Betriebsärzte, Sicherheitsingenieure und andere Fachkräfte für Arbeitssicherheit"

⇒UVV "Arbeitsmedizinische Vorsorge"

Die tätigkeitsbezogenen Unfallverhütungsvorschriften werden für solche Tätigkeiten und Arbeitsbereiche erlassen, bei denen die Arbeitnehmer besonderen Gefahren ausgesetzt sind und die Beachtung der Basis-Unfallverhütungsvorschriften als Schutz nicht ausreicht. Sie ersetzen aber die Basis-Unfallverhütungsvorschriften nicht, sondern ergänzen diese nur für spezielle Tätigkeitsbereiche.

Die Mindestanforderungen, die bei Herstellung, Ausstattung und Betrieb bestimmter Anlagen und Maschinen zu berücksichtigen sind, sind Gegenstand der objektbezogenen Unfallverhütungsvorschriften. Diese beinhalten auch Vorschriften für das Verhalten der Versicherten, die mit diesen Anlagen und Maschinen in Berührung kommen. Auch sie ersetzen die Basis-Unfallverhütungsvorschriften nicht, ebenso wenig die tätigkeitsbezogenen Unfallverhütungsvorschriften, sondern ergänzen diese nur in dem Fall, dass solche Anlagen oder Maschinen in dem Betrieb verwendet werden.

Alle die genannten Unfallverhütungsvorschriften gelten nur für die Unternehmen und Versicherten der erlassenden Berufsgenossenschaft/des Versicherungsträgers. Um das Schutzniveau für alle Beschäftigten gleich zu halten, ist es daher notwendig, dass alle Versicherungsträger im wesentlichen inhalts- sowie zeitgleich die Unfallverhütungsvorschriften erlassen. In der Regel wird in den Unfallverhütungsvorschriften darauf verzichtet konkrete technische Regelungen zu treffen; es wird auf DIN-Normen, VDE-Bestimmungen etc verwiesen.

8.1.3 Technische Normen

Technische Normen (z.B. DIN-Normen, VDE-Bestimmungen), besser gesagt, deren Inhalt, besitzen einen rechtsverbindlichen Charakter nur in ganz bestimmten Fällen.

Solch ein Fall wäre z.B., wenn in einer `dynamischen Verweisung´ in einer Rechtsnorm (Gesetz, Verordnung) auf eine oder mehrere Normen verwiesen wird. Die darin erwähnten Normen würden nun einen rechtsverbindlichen Charakter besitzen; dies wird jedoch als verfassungsrechtlich unzulässig betrachtet. (Zu den genauen Problemen und juristischen Feinheiten vgl. Bar, S. 64 ff.) Daher wird oft eine statische Verweisung gewählt, d.h. es wird auf eine durch das Ausgabedatum konkretisierte Fassung der Norm verwiesen. Aber nur der Inhalt der Norm ist dadurch rechtsverbindlich.

In der sogenannten Inkorporation wird die Norm ganz oder auszugsweise wörtlich in die Rechtsnorm übernommen. Auch in diesem Fall erhält die Norm selbst keinen Rechtssatzcharakter.
Es ist aber trotzdem auch im allgemeinen (d.h. auch wenn die Normen bzw. deren Inhalt keinen rechtlich verbindlichen Charakter haben) sehr wichtig, einschlägige Normen zu beachten. In vielen Bereichen der Sicherheitstechnik besteht mittlerweile ein faktischer Zwang, sich nach den Normen zu richten (z.B. Schutzschuhaufbau, Maschinenschutzeinrichtungen, Bildschirme, elektrische Verbindungsteile etc.). Normen gelten als anerkannte Regeln der Technik. Bei Streitfällen griffen und greifen Gerichte i.d.R. auf Normen zurück, wenn es darum geht zu beurteilen, ob eine Lieferung oder Leistung fehlerhaft war, ob eine Gerät, Maschine oder Anlage sicher genug war/ist oder ob jemandem, der z.B. an einem Unfall mehr oder weniger aktiv beteiligt war, Fahrlässigkeit vorzuwerfen war/ist.
Daher wird/wurde auch in diesem Buch oft auf Normen verwiesen, z.B. im Kapitel 3, in welchem Soft- und Hardwareergonomie besprochen wird.

8.2 Unfalldatenerfassung, Termini der Unfallanzeige

Eines der wichtigsten Module dieser Programme ist der Unfalldatenerfassungsteil. Hier richten sich die Hersteller der Programme in der Regel nach den Vorgaben der Berufsgenossenschaften und haben den Inhalt des Unfallmeldeformulars oft unverändert übernommen.
Dieses Formular wurde von der Bundesanstalt für Unfallforschung entwickelt. Auf einer DIN A4-Seite enthält es alle wichtigen Daten des Verunfallten als auch alle aus versicherungsrechtlichen Gründen notwendigen Informationen zur Verletzung und zum Unfallhergang - falls es sorgfältig und gewissenhaft ausgefüllt wird.

8.2.1 Allgemeine Betrachtungen zur Unfalldatenerfassung

Es wird oft kritisiert, dass die Daten des Unfallmeldeformulars für die Unfallursachenforschung nicht ausreichend sind (vgl. u.a. Ski, S. 49; Rehs, S. 35). Dies ist richtig, liegt aber im eigentlichen Ziel `Schadensmeldung´ des Formulars begründet. Die Hersteller von Programmen zur Unfalldatenerfassung haben das Problem, dass der Kunde möglichst schnell und bequem die Daten eingeben will und im allgemeinen nicht daran interessiert ist, mehr als nötig einzugeben. In der Regel hat eine FaSi auch nicht die Zeit, weitere - für die eigentliche Unfallmeldung unnötige - Daten einzugeben.
Um das Ziel schnelle und bequeme Dateneingabe zu erreichen, ist bei den meisten Programmen dieser Teil so komfortabel wie nur irgend möglich gehalten. Für die Eingaben, für die dies möglich ist, sind Auswahl-Menüs (oft als Pull-down-Feld) vorgegeben. Wenn man etwas Routine besitzt, kann man so

die Daten fast schneller in den Rechner eingeben als ein Unfallmeldeformular von Hand auszufüllen.
Es gibt einige Programme, die eine weitergehende Datenaufnahme ermöglichen, um die Unfallursachenforschung zu stützen. Aber diese Möglichkeit wird vom Kunden nur selten genutzt. "Es lohnt sich nicht, für so etwas viel Zeit zu `verschwenden´, wenn die Sachlage ohnehin klar ist," ist ein häufiges Argument der Praktiker. Hier würde die Eingabe weiterer Daten jedoch die Möglichkeit geben, sich Selbst zu fragen, ob man nicht doch was Wichtiges übersehen hat. Dazu kommt folgende Frage: "Wer weiß aber ein halbes Jahr später noch genau, was da eigentlich exakt passiert war?"
Für Wissenschaft und Forschung wäre es sehr wichtig, über weitergehende Daten zu verfügen. Zusammenfassungen und betriebliche Statistiken haben den Nachteil, dass die Daten oft mehrfach und nach unterschiedlichen Kriterien verdichtet sind. Aber auch das zur Verfügung stellen von ausgefüllten Unfall-anzeigen und Verbandbucheintragungen hat aufgrund der eingeschränkten Daten nur einen begrenzten Wert. Dazu kommt das Problem, dass die Daten uninterpretiert sein müssen. Fehleinschätzungen durch die aufnehmende Person sollten zwar durch gute Kategorisierung vermieden werden, aber lassen sich nicht immer vermeiden. Und die Daten selbst aufnehmen, ist aus u.a. finanziellen Gründen für den Hochschulforscher fast unmöglich, denn das Unfallgeschehen hat einen stochastischen Charakter, so dass man nicht an einem bestimmten Ort warten kann, bis ein Unfall `endlich´ geschieht.

8.2.2 Inhalt des Unfallmeldeformulars (der Unfallanzeige)

Die Unfallanzeige beinhaltet alle Informationen, die für den Versicherer notwendig sind, um die etwaigen Ansprüche des Verletzten, im wohl schlimmsten Fall seiner Hinterbliebenen, zu regulieren. Die Daten der Unfall-anzeigen bilden auch die Grundlage für statistische Auswertungen der Un-falldaten durch die gewerblichen Berufsgenossenschaften. Diese Auswertungen sind Teil des jährlichen Unfallverhütungsberichtes der Bundesregierung.
Das Unfallmeldeformular beinhaltet 41 Unterpunkte. Diese sind gegliedert in einen Verwaltungsteil, in Angaben zum Verletzten, Angaben zur Verletzung und Angaben zum Unfall:
"Das erste auszufüllende Feld beinhaltet die Frage nach der Mitgliedsnummer des Unternehmens bei dem zuständigen Unfallversicherungsträger, im zweiten muss das Gewerbeaufsichtsamt bzw. Bergamt angegeben werden, im dritten die Betriebsnummer des Arbeitsamtes und im vierten befindet sich Raum für die Anschrift des Empfängers der Unfallanzeige. Diese Punkte bilden den ersten Abschnitt des Formulars, den verwaltungstechnischen Teil.
Es folgen nun die Angaben zum Verunfallten. Hier wird zunächst der Name, der Vorname, die Versicherungsnummer oder das Geburtsdatum und die

Adresse abgefragt (Punkte 5 - 7), um eine eindeutige Identifizierung zu gewährleisten. Für die versicherungstechnische Arbeit sind folgende Daten von Bedeutung:
Der Familienstand, das Geschlecht, die Staatsangehörigkeit und die Zahl der Kinder unter 18 Jahren (bzw. zwischen 18 und 25 Jahren, sofern sich diese noch in der Berufsausbildung befinden) (Punkte 8 - 11).
Die nächsten drei Punkte beziehen sich auf die Tätigkeit des Verunfallten und seine Erfahrungen in diesem Gebiet. Der folgende Fragenblock gibt dem Unfallversicherer Auskünfte über die von ihm zu tragenden Leistungen. Es sind Angaben zu machen, ob er minderjährig oder entmündigt ist (evtl. Angabe des gesetzlichen Vertreters), ob er der Unternehmer selbst ist oder in einem verwandtschaftlichen Verhältnis zu diesem steht. Auch die verantwortliche Krankenkasse muss eingetragen werden (Punkte 15 - 18). Die letzten Fragen in diesem Abschnitt sind nach dem zeitlichem Rahmen des `Anspruches auf Arbeitsentgelt´ und nach dem Zeitpunkt der `Wiederaufnahme der Arbeit´ (Punkte 19, 20).
Im anschließenden Fragenblock werden Angaben zur Verletzung verlangt. Im einzelnen sind dies:

21) verletzte Körperteile
22) Verletzungsart
23) zuerst behandelnder Arzt (Name, Anschrift)
24) Unfall mit Todesfolge
25) zur Zeit behandelnder Arzt (Name, Anschrift)
26) Krankenhaus

Mit Hilfe dieser Informationen kann der Unfallversicherungsträger zum einen leicht Recherchen durchführen, zum anderen dienen diese Angaben statistischen Zwecken (spez. 21, 22, 24).
Der letzte Abschnitt beinhaltet Fragen zum Unfallhergang. Zunächst müssen der genaue Unfallzeitpunkt und der Zeitpunkt des Einstellens der Arbeit eingetragen werden (Punkte 27, 28), dann werden Angaben über die normale Arbeitszeit verlangt. Nun folgen Fragen zur exakten Unfallstelle, zum Unfallgegenstand, zu vorhandenen technischen Schutzvorrichtungen und benützten persönlichen Schutzvorrichtungen, sowie nach zukünftigen Schutzmaßnahmen (Punkte 31 - 35). Die abschließenden Angaben bilden Name und Anschrift von möglichen Zeugen und ausführliche Schilderung des Unfallhergangs.
Das Formular bietet nun noch Raum für das Datum und die Unterschriften der über das Geschehen zu informierenden, verantwortlichen Personen (Unternehmer/Stellvertreter, Betriebsrat/Personalrat, Sicherheitsbeauftragter).”
/Wic, S. 26-28/

Die Punkte 31 bis 35 sowie 37 sind für die Unfallursachenerforschung interessant. Wie uns verschiedene Forschungsprojekte zeigten, werden diese Fragen oft nur knapp und ungenau beantwortet. Insbesondere die Frage 37 `Ausführliche Schilderung des Unfallherganges´, die eigentlich Raum bieten würde, das Unfallgeschehen genau zu beschreiben, wird oft in nur zwei oder drei Stichworten beantwortet. Dies kann vielleicht mit dem Versicherungszweck des Formulars begründet werden. Wer gefährdet schon gerne den Versicherungsschutz des Unternehmens und damit des Betroffenen, indem er Stichpunkte liefert, die dem zuständigen Versicherungsträger (in der Regel einer Berufsgenossenschaft) möglicherweise Anlass bieten, genauere Nachforschungen zu betreiben.

8.3 Statistische Grundlagen, Unfallkennzahlen

Als eine Erleichterung, welche die Unfalldatenerfassungs- und –bearbeitungsprogramme bieten, wird oft der statistische Teil erwähnt. Die meisten Programme bieten auch die Möglichkeit die gängigen statistischen Kennzahlen bzw. die üblichen Unfallkennzahlen bequem zu ermitteln und graphisch darzustellen. Um diesen Programmteil ausnützen zu können, ist es notwendig, über die grundlegenden statistischen Kenntnisse zu verfügen und die einzelnen Unfallkennzahlen zu kennen.

8.3.1 Deskriptive Statistik

Die Statistik wird gewöhnlich als Methodenlehre definiert, welche die Ergebnisse von Beobachtungen (Messungen, Zählungen etc.) darstellt und zusammenfasst. Unterschieden werden: deskriptive und induktive Statistik.

Man bezeichnet die deskriptive Statistik auch als beschreibende Statistik. Sie hat die Aufgabe, in der Regel unübersehbare Datenmengen zu ordnen und durch möglichst wenige, aber aussagekräftige Zahlen übersichtlich darzustellen. Man unterscheidet quantitative und qualitative Merkmale. Quantitative Merkmale sind z.B. Alter, Dauer der Betriebszugehörigkeit und lassen z.B. die Bildung eines sinnvollen Mittelwertes zu.

Qualitative Merkmale sind u.a. Berufsbezeichnung, Wohnort etc. Auch diese Merkmale werden oft quantifiziert, d.h. als Zahlenwerte dargestellt. Aber es kann kein sinnvoller Mittelwert gebildet werden.

Das Datenmaterial kann ein- oder mehrdimensional ausgewertet werden. Folgende Kenngrößen können bei eindimensionaler (d.h. nur ein Merkmal wird berücksichtigt) Auswertung ermittelt werden /vgl. hierzu die sicherheitstechnische Anwendung bei Schulz, S. 69 ff./:

⇒*Häufigkeitsverteilung*
Man unterscheidet absolute und relative Häufigkeitsverteilung. Zur graphischen Darstellung benutzt man oft Stabdiagramme, Kreissektorendiagramme und Histogramme bei klassifizierten Daten.

⇒*Lageparameter*
“Zu den Lageparametern zählen der Modalwert (oder häufigster oder dichtester Wert), der Median (oder Zentralwert), das arithmetische Mittel (im Alltag meist als Durchschnittswert bezeichnet) und das geometrische Mittel. Diese statistischen Größen sollen anhand eines einfachen Beispiels veranschaulicht werden:
Ausgegangen werden soll von 6 Unfällen mit 30, 11, 22, 69, 7 und 5 Ausfalltagen. Das arithmetische Mittel der Ausfalltage (mittlere Anzahl von Ausfalltagen) wird dadurch ermittelt, dass die Ausfalltage der einzelnen Unfälle addiert werden und diese Summe durch die Anzahl der Unfälle dividiert wird:

Mittelwert: $$\overline{X} = \frac{\sum_{i=1}^{n} x_i}{n}$$

Mit den Zahlen aus dem Beispiel wird ein Mittelwert von 24 Tagen Ausfallzeit ermittelt:

$$\overline{X} = \frac{30 + 11 + 22 + 69 + 7 + 5}{6} = 24$$

Hat sich zusätzlich noch ein tödlicher Unfall ereignet, der mit einer sehr hohen Zahl von Ausfalltagen (z.B. 7500 Tage; vgl. dazu Schulz, S. 70) bewertet wird,

dann liegt das arithmetische Mittel der Ausfalltage erheblich höher:

$$\overline{X} = \frac{144 + 7500}{7} = 1092$$

Die Auswirkung von extremen Werten wird vermindert, wenn statt des arithmetischen Mittelwertes der Median herangezogen wird. Dazu werden die vorliegenden Werte - im Beispiel die Zahlen der Ausfalltage - aufsteigend sortiert und der Wert genommen, der in der Mitte dieser Reihe liegt /Hei, S.19/:

Median:

$$X_{0,5} = \begin{cases} X_{k+1} & \textbf{fuer n = 2 k + 1} \\ \dfrac{X_k + X_{k+1}}{2} & \textbf{fuer n = 2 k} \end{cases}$$

Mit den obigen Zahlen ergibt sich die Reihenfolge 5, 7, 11, 22, 30, 69, 7500 und damit ein Median von 16,5 ohne bzw. 22 mit dem tödlichen Unfall. Der Median ist unabhängig davon, wie hoch die Ausfallzeit nach einem tödlichen Unfall bewertet wird, solange sie größer ist als die Ausfallzeit jedes anderen Unfalls.
Bei größeren Datenmengen sind einzelne Werte oft mehrfach vertreten. Diese werden dann z.B. in einer Häufigkeitstabelle (siehe Tab. 8.2-1) zusammengefasst. Am häufigsten vertreten sind in diesem Beispiel 7 Ausfalltage bei 18 Unfällen. Dieser Wert (d.h. 7 Unfalltage) wird als Modalwert bezeichnet und ist - wie der Median - unabhängig von extremen Werten.

Ausfalltage	Zahl der Unfälle
5	7
7	18
11	12
30	5
69	1

Tabelle 8.2-1 Häufigkeitstabelle

Liegt eine Häufigkeitsverteilung vor, dann muss die Definition des arithmetischen Mittelwertes dahingehend erweitert werden, dass die Häufigkeiten h_i berücksichtigt werden. Der so erhaltene Wert wird als gewogenes Mittel bezeichnet" /Pat, S. 10 -12/:

gewogenes Mittel: $\overline{x} = \dfrac{\sum_{i=1}^{n} x_i h_i}{\sum_{i=1}^{n} h_i}$

⇒*Streuungsparameter*

"Streuungsparameter sind die Spannweite, die durchschnittliche Abweichung, die mittlere quadratische Abweichung (oder Varianz), die Standardabweichung und der Variationskoeffizient.

Die Streuungsparameter geben Aufschluss darüber, wie weit die einzelnen Werte voneinander entfernt sind. Die Spannweite gibt lediglich den Abstand zwischen dem höchsten und dem niedrigsten Wert an:

Spannweite: $R = x_{max} - x_{min}$

Mit den Zahlen aus Tabelle 8.2-1 ergibt sich eine Spannweite von
69 -5 = 64 Ausfalltagen.

Als Streuungsparameter wird meist die Varianz eingesetzt /vgl. Hei, S. 24/, die ein Maß dafür ist, `wie stark die Beobachtungen durchschnittlich von ihrem Mittelwert abweichen.´ /Sac, S. 19/:

Varianz: $s^2 = \dfrac{\sum_{i=1}^{n} (x_i - \bar{x})^2}{n - 1}$

Mit den Zahlen aus dem Beispiel ergibt sich folgende Rechnung:

$S^2 = [(30 – 24)^2 + (11 – 24)^2 + (69 – 24)^2 + (7 –24)^2 + (5-24)^2] / [6 – 1]$
$= (36 + 169 + 2025 + 289 + 361) / 5 = 2884 / 5 = 576,8$

Da die Varianz als quadratisches Streumaß oft unanschaulich ist, wird statt dessen meistens die Standardabweichung eingesetzt /Hei, S. 25/:

Standardabweichung $S = \quad S^2$

Ein weiterer Streuungsparameter ist der Variationskoeffizient, der z.B. dann berechnet wird, wenn angenommen wird, dass die Standardabweichung und das arithmetische Mittel proportional sind. /Hei, S. 26/:" /Pat, S. 12 - 14/

Variationskoeffizient $VK = S / \overline{X}$

⇒Konzentrationsmaße

Diese werden in der Regel verwendet, um Konzentrationstendenzen darzustellen. Oft wird das Konzentrationsmaß von Lorenz als grafisches Hilfsmittel eingesetzt. /vgl. Bam, S. 24/

"Mehrdimensionale Auswertungen sollen einseitige oder wechselseitige Abhängigkeiten aufdecken. Die dafür einsetzbaren Methoden sind die Korrelations- und die Regressionsrechnung. Der Korrelationskoeffizient ist ein Maß für den Grad der linearen Abhängigkeit zwischen zwei quantitativen, metrisch gemessenen Merkmalen. /Hei, S. 32/ Besteht zwischen zwei Merkmalen x und y ein Zusammenhang, dann gibt der Regressionskoeffizient an, um wie viel Maßeinheiten sich die Zielgröße y verändert, wenn sich die Einflussgröße x um eine Maßeinheit ändert." /Pat, S. 14/

Mehr soll an dieser Stelle zur deskriptiven Statistik nicht geschrieben werden, da die Unfalldatenbearbeitungsprogramme gewöhnlich keine weitergehenden Kenngrößen (z.B. Indexzahlen, Saisonbereinigung) anbieten. Es stellt sich hier aber auch die Frage, ob eine weitere Vertiefung für die betriebliche Praxis einen Sinn hätte. Wenn es sich nicht gerade um Konzerne handelt, ist das Unfallvorkommen wohl oft zu gering, um weitergehende deskriptive statistische Auswertungen zu rechtfertigen.

8.3.2 Induktive Statistik

Die induktive Statistik wird auch als analytische, beurteilende, schließende oder Inferenzstatistik bezeichnet. Sie findet Anwendung, wenn z.B. eine vollständige Datenerhebung nicht möglich ist oder aus verschiedenen Gründen als nicht zweckmäßig erscheint. Es werden in solchen Fällen Stichproben genommen und aus den so erhaltenen Daten Rückschlüsse auf die Grundgesamtheit gezogen. Auch wird diese Methode gerne genommen, um die Gültigkeit von Hypothesen bezüglich der Grundgesamtheit zu überprüfen. Für die Stichprobe gilt, dass sie die Gesamtheit, aus der sie stammt, gut widerspiegeln soll, also \`repräsentativ´ ist. /vgl. hierzu Hei, S.82 f./

In der Praxis wird zwischen zufälligen und nichtzufälligen Stichproben unterschieden:

⇒Nichtzufällige Stichproben
Hier unterscheidet man die \`Auswahl aufs Geratewohl´, die \`Methode der typischen Fälle´ und die \`bewusste Auswahl´.
Bei der bewussten Auswahl versucht man, eine möglichst repräsentative Stichprobe zu erhalten. Beispiele sind das Quotaverfahren und die Konzentrationsstichprobe, die gerne angewendet werden.
Nachteilig bei einer nichtzufälligen Stichprobe ist, dass der Stichprobenfehler fast nicht abgeschätzt werden kann. Ein Stichprobenfehler ist unvermeidbar, da nur ein Teil der gesamten statistischen Daten untersucht wird.

⇒Zufällige Stichproben
“Bei zufälligen Stichproben wird die Auswahl der Elemente durch einen Zufallsmechanismus bestimmt. /Hei, S. 83/ Die Auswahlverfahren für zufällige Stichproben sind:
* Reine oder uneingeschränkte Zufallsstichprobe
Durch Würfeln oder Auslosen oder unter Verwendung von Zufallszahlentafeln werden aus der Grundgesamtheit Teilmengen gebildet. /Hei, S. 83 f./ Jedes Element der Grundgesamtheit hat für die Auswahl die gleiche Wahrscheinlichkeit. Als Behelf einer reinen Zufallsauswahl finden die systematische und die Buchstaben- oder Geburtstagsauswahl Anwendung. Bei der systematischen Auswahl wird z.B. aus einer Kartei jedes k-te Element, beginnend bei einem zufälligen Startpunkt, ausgewählt. Für die Buchstaben- oder Geburtstagsauswahl werden Personen ausgewählt, deren Name mit einem bestimmten Buchstaben beginnt oder die an einem bestimmten Tag Geburtstag haben. Zu dieser Kategorie zählen die Unfallstatistiken vieler Berufsgenossenschaften, die alle Merkmale der Unfallanzeigen nur für Personen auswerten, die am 10./11./12. eines Monats geboren wurden, woraus sich eine Stichprobe von 10% ergibt. /vgl. Beispiele hierzu bei Hoff, S. 8/
* Geschichtete Stichprobe
Wenn bekannt ist, dass gewisse Teilgesamtheiten, die als Schichten bezeichnet werden, bezüglich des Untersuchungsmerkmals besonders homogen sind, dann werden die Elemente der Stichprobe nicht mehr durch eine reine Zufallsauswahl bestimmt. /Bam, S. 242/ Statt dessen wird der Stichprobenumfang in geeigneter Weise auf die Schichten aufgeteilt. Der dadurch gegenüber der reinen Zufallsauswahl erzielte Genauigkeitsgewinn wird als Schichtungseffekt bezeichnet. Eine geschichtete Stichprobe liegt zum Beispiel dann vor, wenn bei einer Einkommensuntersuchung eine Aufteilung in Berufsgruppen erfolgt. /Hei, S. 84/

* Klumpenstichprobe
Die Klumpenstichprobe stellt ebenso wie die geschichtete Stichprobe eine Klasseneinteilung der Gesamtheit dar. /Hei, S. 85/ Die Klumpenbildung erfolgt vor allem durch geographische, soziologische oder zeitliche Abgrenzung (z.B. durch Aufteilung in Haushalte oder Familien, Gemeinden, Häuserblöcke, usw.) und wird hauptsächlich zur Einsparung von Kosten (Interviewer-, Reisekosten, usw.) durchgeführt. Der Kostenminderung steht ein als Klumpeneffekt bezeichneter Genauigkeitsverlust der Schätzung gegenüber. Eine regionale Klumpenbildung wird als Flächenstichprobe bezeichnet." /Pat, S. 16 -18/
Für die Arbeit mit den gängigen Unfalldatenbearbeitungsprogrammen ist die Kenntnis der hier genannten und beschriebenen statistischen Methoden ausreichend, denn mehr statistische Arbeitsmöglichkeiten stellen die Unfalldatenbearbeitungsprogramme in der Regel nicht zur Verfügung. Sollte man doch mehr Informationen zu statistischen Methoden benötigen, können die Bücher von Bamberg/Baur und Heiler/Rinne empfohlen werden. Diese sind sehr gut verständlich und bieten anschauliche Beispiele.

8.3.3 Unfallkennzahlen

In der Sicherheitstechnik werden zur Beschreibung des Schadensausmaßes des Unfallvorkommens in der Arbeitswelt verschiedene relative (Unfall-) Kennzahlen verwendet. Diese Kennzahlen können für Vergleiche der Unfallvorkommen verschiedener Betriebe oder auch ganzer Berufsgenossenschaften benutzt werden (Beispielsweise im Unfallverhütungsbericht der Bundesregierung). Die Kennzahlen, die im folgenden vorgestellt werden, sind auf den Menschen bezogen. Sie werden angewendet, um die Folgen von Arbeitsunfällen oder Wegeunfällen zu beschreiben.

⇒Die *`1000-Mann-Unfall-Quote´*
"Die 1000-Mann-Unfall-Quote relativiert die Anzahl der Unfallereignisse zur Anzahl der Beschäftigten. Damit kann direkt die Häufigkeit von Unfallereignissen zweier oder mehrerer, auch unterschiedlich großer Gruppen miteinander verglichen werden."/Com-BW, S. 47/

$$\boxed{\text{1000-Mann-Unfall-Quote}} = \frac{\text{Anzahl der Unfaelle * 1000}}{\text{mittlere Belegschaftsstaerke}}$$

Bei der Anwendung dieser Kennzahl können verschiedene Probleme auftreten. Beispielsweise kann die Arbeitszeit des Betroffenen von der des vom Hauptverband der Berufsgenossenschaften als Standard vorgegebenen Vollarbeiters abweichen (u.a. durch Teilzeitarbeit, Schichtdienst, Überstunden). Ebenso muss man sich bei der Verwendung dieser Kennzahl als Vergleichsmaßstab auf gleiche Zeitabschnitte einigen.
"Dies wird an folgendem Beispiel (nach IG-Metall, S. 11) deutlich:
Angenommen, in einem Unternehmen mit 100 Belegschaftsmitgliedern ereignen sich jeden Monat zwei Unfälle, im Jahr also 24 Unfälle. Dann ergeben sich für die 1000-Mann-Unfall-Quote folgende Werte:

monatliche 1000-Mann-Unfall-Quote = 2 * 1000 / 100 = **20**

jährliche 1000-Mann-Unfall-Quote = 24 * 1000 / 100 = **240**

Dieselbe Situation spiegelt sich hier in zwei sehr unterschiedlichen Werten der 1000-Mann-Unfall-Quote wider. Es ist also anzugeben, für welche Zeitspanne (Monat, Quartal, Jahr usw.) die 1000-Mann-Unfall-Quote berechnet wurde, um Fehlschlüssen vorzubeugen.
Ungenauigkeiten treten bei der 1000-Mann-Unfall-Quote vor allem dann auf, wenn diese für relativ kleine Zeiträume (z.B. ein Monat) mit unter-schiedlicher Anzahl von Arbeitstagen angegeben wird." /Pat, S. 60/61/

⇒Der *`Leistungsausfall´*
Ersetzt man im Zähler die Anzahl der Unfälle durch die Summe der (Kalender-) Ausfalltage und hat im Nenner weiterhin die Belegschaftsstärke so erhält man als Kennzahl den Leistungsausfall:

$$\text{Leistungsausfall} = \frac{\sum \text{Kalenderausfalltage}}{\text{mittlere Belegschaftsstaerke}}$$

Mit diesem Wert wird die auf die gesamte Belegschaft verteilte unfallbedingte Ausfallzeit beschrieben. Krause /Krause, S. 77/ vertritt die Meinung, dass dies aus betriebswirtschaftlicher Sicht eine interessante Größe ist. /vgl. Pat, S. 61/

⇒Die *`Unfall-Häufigkeits-Rate´*
"Die Unfall-Häufigkeits-Rate relativiert die Anzahl der Unfallereignisse zur Anzahl der verfahrenen Arbeitsstunden. ... Die Ermittlung der `verfahrenen

Arbeitsstunden´ ist prinzipiell auch für Bereiche möglich, die mit dem Terminus `Vollarbeiter´ nicht arbeiten können." /Com-BW, S. 47/73/

$$\boxed{\text{Unfall-Häufigkeits-Rate}} = \frac{\textbf{Anzahl der Unfaelle} * 10^6}{\textbf{geleistete Arbeitsstunden}}$$

"Diese Kennzahl ist besonders für Betriebsvergleiche geeignet, sie gilt als zuverlässig und aussagehaltig, da sie die sog. Gefahrenexposition anhand der Arbeitstunden ausdrückt." /Pilz, S. 83/

⇒Die *`Gefährdung´*
Die als Gefährdung bezeichnete Kennzahl ist definiert als die Summe der Kalender-Ausfalltage, die auf 1000 geleistete Arbeitsstunden bezogen werden:

$$\boxed{\text{Gefährdung}} = \frac{\sum \textbf{Kalenderausfalltage} * 1000}{\textbf{geleistete Arbeitsstunden}}$$

Nach Krause lässt die Kenngröße Gefährdung auf die relative Höhe von Gefahren schließen, wenn für das Wirksamwerden dieser Gefahren gleiche Wahrscheinlichkeiten angenommen werden. Durch die nicht konstanten Auswirkungen des (unterschiedlichen) menschlichen Verhaltens wird die Aussagekraft der sogenannten `Gefährdung´ als Kenngröße vermindert. /Krause, S. 78/

⇒Die *`Unfall-Schwere-Rate´*
"Die `Unfall-Schwere-Rate´ bezieht die unfallbedingten Ausfallstunden auf die verfahrenen Arbeitsstunden." /Com-BW, S. 49/

$$\boxed{\text{Unfall-Schwere-Rate}} = \frac{\sum \textbf{Ausfallstunden} * 100\,000}{\sum \textbf{Arbeitsstunden}}$$

Pilz bezeichnet die gleiche Kennzahl als Unfallausfallrate. /Pilz, S. 83/
⇒Die *`Schwerpunktkennzahl´*
Eine Kennzahl, die für die Unfallforschung zur Feststellung von besonderen Gefährdungen geeignet scheint, ist die Schwerpunktkennzahl. Hier werden die

Unfallschwere (durch die Ausfalldauer in Tagen) und die Risikodauer (durch die Expositionszeit) erfasst und miteinander in Beziehung gesetzt.

$$\text{Schwerpunktkennzahl} = \frac{\sum \text{Ausfallstunden}}{\text{Expositionszeit}}$$

Problematisch ist hier jedoch die Quantifizierung der Expositions- bzw. Risikodauer. Für die praktische Anwendung sieht Thiele die Anzahl der verfahrenen Arbeitsstunden als bestgeeignete Größe für die Expositionsdauer an. /vgl. Pat, S. 64/

⇒Die *`durchschnittliche Verletzten-Ausfalldauer´*
“Die `durchschnittliche Verletzten-Ausfalldauer´ betrachtet die unfallbedingten Ausfallzeiten in Relation zur Anzahl der Unfälle.” /Com-BW, S. 49/ Krause bezeichnet die gleiche Kennzahl als `Unfallschwere´. /Krause, S. 77/

$$\text{Durchschnittliche Verletzten-Ausfalldauer} = \frac{\sum \text{unfallbedingte Ausfallzeiten}}{\sum \text{meldepflichtige Unfaelle}}$$

In der Regel wird die Ausfallzeit in Kalendertagen angeben. Es wird die Zeitspanne vom Tag nach dem Unfall bis zum Tag vor der Wiederaufnahme der Arbeit betrachtet. Es werden oft aber auch die Ausfallstunden benutzt oder andere Abweichungen von der Regel gemacht, so dass man sich bei Vergleichen von Statistiken verschiedener Herkunft über den Inhalt des Zählers `Ausfallzeit´ einigen muss.

Allen diesen Kennzahlen ist gemeinsam, dass sie für die Arbeit zur Erforschung von Methoden und Maßnahmen zur Unfallverhütung nur einen begrenzten Nutzen haben. Sie gehen weder auf die Art der Verletzung ein, noch auf den eigentlichen Unfallhergang selbst, noch werden die Gegenstände berücksichtigt, die beim Unfallgeschehen beteiligt waren und/oder beschädigt bzw. zerstört wurden. Interessant wären bestimmt auch Kennzahlen, welche die finanziellen Auswirkungen eines Arbeitsunfalls beschreiben. Die hier beschriebenen Kennzahlen berücksichtigen weder die finanziellen Aspekte einer

Verletzung, noch werden die sonstigen materiellen Folgen (z.B. zerstörte Gegenstände, Produktionseinbußen) eines Arbeitsunfalls betrachtet.

8.4 Unfallstatistik, Termini der Unfallstatistik

"Wie bei jeder Statistik, so erfolgt auch die Erstellung der Unfallstatistik in zwei Schritten: Beschaffung des Datenmaterials und Aufgliederung dieses Materials zu einer anschaulichen Übersicht (Pilz, S. 79). Dabei ist zu berücksichtigen, dass die Statistik nicht als Selbstzweck dient, sondern Arbeitsmittel ist. Als Konsequenz daraus folgt, dass die Datenbeschaffung der wichtigere Teil der Statistik ist. Für die Unfallstatistik bedeutet dies, dass nur gründlich untersuchte Unfälle zu einer aussagekräftigen Unfallstatistik führen, mit deren Hilfe Impulse für die betriebliche Arbeitssicherheit gewonnen werden können. Während die Auswertung der Daten in früheren Jahren hauptsächlich auf `das Auszählen der Häufigkeit der einzelnen Merkmale ..., das Feststellen ihrer Verteilung, ggf. die Relativierung mit anderen Betriebsgrößen und die Interpretation der Ergebnisse´ (Krause, S. 73) beschränkt war, lassen sich mit den Mitteln der heutigen Datenverarbeitungsanlagen zusätzliche Abhängigkeiten zwischen mehreren Merkmalen ableiten.
Bevor eine Statistik aufgestellt wird, ist es sinnvoll festlegen, welchen Zweck sie erfüllen soll (Pilz, S. 80). Für die Unfallstatistik ergibt sich im wesentlichen eine Gliederung in zwei Gruppen." /Pat, S. 20 und 21/

8.4.1 Berichtsstatistik

"Die Berichtsstatistik erfasst den Stand und die Entwicklung des Unfall-vorkommens und macht deutlich, in welchen Bereichen besondere Maßnahmen im Rahmen der Unfallverhütung zu treffen sind (Kronauer, S. 105). Um Vergleiche zwischen den einzelnen Betrieben, Betriebsstellen oder Unternehmen durchführen zu können, werden die ermittelten absoluten Zahlen mit Kenngrößen in Beziehung gesetzt (Krause, S. 73) und dadurch relativiert. Dazu ist es notwendig, die in der Berichtsstatistik verwendeten Begriffe eindeutig gegeneinander abzugrenzen, um Auslegungsspielräume zu vermeiden." /Pat, S. 21/

8.4.2 Arbeitsstatistik

"Die Arbeitsstatistik dient dazu, Informationen über Möglichkeiten zur Be-einflußung des Unfallgeschehens zu liefern (Krause, S. 103). Besonders wichtig bei der Arbeitsstatistik ist, dass jede Zahlenangabe ohne großen Aufwand bis zu ihrem Ursprung zurückverfolgt werden kann (Pilz, S. 81). Nur dadurch kann sichergestellt werden, dass die Arbeitsstatistik ihrem Zweck gerecht wird, ein brauchbares Hilfsmittel für die Unfallforschung zu sein." /Pat, S. 22/

8.4.3 Merkmale zu den Umständen des Unfalls

Mit Hilfe statistischer Auswertungen der Unfallanzeigen und der Verbandbucheintragungen können verschiedene Merkmale festgestellt werden, die Anhaltspunkte für die Unfallursache beinhalten können, die den Unfallhergang beschreiben und die Unfallfolgen schildern. Einige der im folgenden erwähnten Punkte sind jedoch mehr aus versicherungstechnischen Gründen interessant und werden daher nicht weiter besprochen.

Geht man auf die Umstände des Unfalles ein, unterscheidet man in der Regel zwischen ortsgebundenen, zeitgebundenen, personengebundenen Umständen.

Bei den ortsgebundenen Umständen werden u.a. Wirtschaftszweig und Betriebsgröße angegeben, liefern aber für die Unfallursachenforschung an sich keine Erkenntnisse. Unfallort, Arbeitsbereich und Arbeitsablauf, Wetter und Arbeitsklima sind Umstände, die einen Unfall auslösen und einen Unfallhergang beeinflussen können. Auch die ergonomischen Umstände als auch die Arbeitsschwere können für die Unfallursachenforschung interessant sein.

Insbesondere bei Arbeiten im Freien kann das Wetter im Unfallgeschehen eine wichtige Rolle spielen. Glätte, Nässe, Hitze aber auch `nur´ unpassende/ungeeignete Kleidung können direkt zu Unfällen führen. In geschlossenen Räumen kann sich das Wetter ebenfalls auswirken; es gibt genügend Menschen, die z.B. bei Wetterumschlag mit Kopfschmerzen, Konzentrationsschwäche o.ä. zu kämpfen haben. Es ist oft so, dass das Klima am Arbeitsplatz vom Außenklima abweicht. Dies kann sich insbesondere bei Hitze- und Kältearbeitsplätzen für den Menschen negativ auswirken. Temperatur, relative Feuchte, Luftgeschwindigkeit und Wärmestrahlung sind an Hitze- und Kältearbeitsplätzen aber auch z.B. an Rechnerarbeitsplätzen in bestimmten Grenzen zu halten - im allgemeinen aus Rücksicht auf das Material und ohne Rücksicht auf den Menschen. Wenn sich beide Interessen zufällig treffen, wird dies ausgenützt, ansonsten werden üblicherweise Erschwerniszuschläge gezahlt.

Arbeitsort, Arbeitsbereiche und Arbeitsabläufe können insbesondere in Betrieben interessant sein, die klar in einzelne Arbeitsbereiche aufgetrennt sind und über eine verfahrenstechnische Gliederung verfügen. In einer Gießerei kann man z.B. die einzelnen Arbeitsschritte gut aufteilen und so vielleicht Unfallschwerpunkte entdecken. In kleinen und mittleren Handwerksbetrieben beispielsweise, in denen eine und dieselbe Person verschiedene Tätigkeiten, vielleicht auch noch an verschiedenen Orten ausführt, werden diese Merkmale in der Regel als unrelevant betrachtet; hier kann der Zufall einen zu großen Einfluss haben.

Die zeitgebundenen Einflüsse auf das Unfallvorkommen wurden schon gründlich untersucht. Es wurden die Wochentage, die Monate und Jahreszeiten, die einzelnen Schichtarten und die Arbeitszeit/-dauer an sich betrachtet. Wenn

man z.B. die Wochentage betrachtet, so ist der Montag absolut gesehen der Tag an dem die meisten Unfälle geschehen. Skiba /Ski, S. 56/ schreibt hierzu, dass als Ursache eine mangelnde Umstellung von der Freizeit auf die Arbeit einerseits vermutet wird; andererseits treten erhöhte technische Gefahren auf, wenn die technischen Arbeitsmittel nach Stillstand am Wochenende Instandgehalten und wieder in Betrieb genommen werden. Er vertritt die Auffassung, dass dieses Merkmal keine wesentliche Bedeutung für die betriebliche Unfallverhütung hat.
Ähnliches gilt für Arbeitszeit/-dauer. Es werden auch hier Unfallspitzen zu bestimmten Zeiten festgestellt (z.B. in der Zeit von 10 - 11 Uhr und um ca. 15 Uhr), aber dies wird z.B. mit dem Wechsel der physiologischen Leistungsbereitschaft einerseits sowie dem üblichen Tätigkeitsprofil andererseits recht einleuchtend erklärt. Bei der Schichtarbeit, insbesondere der Wechselschicht tritt eine Störung im gesamten Lebensrhythmus betroffener Arbeitnehmer auf. Das zur Verfügung stehende Zahlenmaterial lässt jedoch keine eindeutigen Rückschlüsse zu, die für die praktische Unfallverhütung von Interesse sind. Z.B. ergab eine Untersuchung, die im Rahmen eines Forschungsprojektes in der chemischen und Eisen- und Stahlindustrie durchgeführt wurde, dass das Unfallvorkommen absolut gesehen in der Frühschicht am höchsten und in der Nachtschicht am niedrigsten war. /Wer, S. 166/ Der Autor dieser Studie betont jedoch, dass diese Zahlen keinen Aufschluss darüber geben, welche Schicht am gefahrträchtigsten ist. Es lagen nämlich keine Angaben zur Schichtbesetzung und zur Arbeitsbelastung des Einzelnen vor. /Wer, S. 166/
Auch ein Einfluss der Jahreszeiten (Monate) lässt sich nachweisen (im Winter die wenigsten, im Herbst die meisten Unfälle), ohne dass brauchbare Folgerungen für die praktische Unfallverhütungsarbeit gezogen werden können. Hier werden die Schwankungen mit den unterschiedlichen Expositionszeiten begründet, die von Auftragsvolumen, Ferienzeiten und der Witterung abhängen. Nach Skiba haben monatliche Auswertungen für den Betrieb nur einen Übersichts-, Vergleich- und Kontrollzweck. /Ski, S. 57/
Lebensalter, Betriebsalter (besser: Betriebszugehörigkeitsdauer), Arbeitsplatzerfahrung, Staatsangehörigkeit, Geschlecht und Beruf werden als personengebundene Umstände betrachtet. Zu Beruf merkt Patrzek an, dass dieses Merkmal in der ihm vorliegenden Literatur wenig in Erscheinung tritt und daher nur für eine Übersichtsstatistik von Interesse ist. /Pat, S. 39/
Im Lebensalter spiegelt sich häufig die Lebens- und Berufserfahrung, der berufliche Werdegang und eine gewisse Routine wieder. Es wurde festgestellt, dass die Unfallhäufigkeit bei jüngeren Arbeitnehmern größer ist als bei älteren Arbeitnehmern, bei älteren Arbeitnehmern nimmt jedoch die Unfallschwere zu. Diese Feststellungen gelten jedoch als nicht sehr aussagekräftig, da unter-

schiedliche Tätigkeiten, verschiedene Ausbildung und unterschiedliche Betriebszugehörigkeitsdauer nicht berücksichtigt wurden.
Mit zunehmender Dauer der Betriebszugehörigkeit wird eine Abnahme der Unfallhäufigkeit festgestellt. Dies wird erklärt mit höherer Erfahrung, persönlicher Anpassung und in der Regel weniger gefährlichen Arbeiten bei längerer Betriebszugehörigkeit. Ähnliches gilt für die Arbeitsplatzerfahrung. Selbst bei einem Arbeitsplatzwechsel im gleichen Betrieb erhöht sich die Unfallgefahr in der ersten Zeit nach dem Wechsel. Hier werden als Gründe angeführt: unangepasstes Verhalten, mangelnde Gewöhnung an die neue Tätigkeit und unzureichende Kenntnisse über die am neuen Arbeitsplatz vorhandenen Gefahren.
Die Zahlen zum Unfallvorkommen bestätigen eigentlich die Auffassung, dass Frauen geschickter bei der Arbeit und weniger anfällig für Monotonie sind. Trotzdem wird einheitlich davor gewarnt, diese Zahlen überzubewerten, da sich Frauenarbeitsplätze in der Regel von Männerarbeitsplätzen grundlegend unterscheiden. /Wup, S. 73; Ski, S. 424/
Auch die Zahlen, die für Ausländer eine relativ höhere Unfallhäufigkeit angeben, lassen sich gut erklären, ohne dass direkt auf Maßnahmen zur Unfallverhütung geschlossen werden kann. Ausländer sind an das (Arbeits-) Leben in Deutschland noch nicht gewöhnt, überwiegend handelt es sich um angelernte Kräfte in Produktionsprozessen und sie müssen oft die unangenehmen und `gefährlichen´ Tätigkeiten durchführen. An diesen (Unfall-) Zahlen lässt sich u.a. sehr gut ablesen, wann eine Einwanderungsphase in Deutschland war.

8.4.4 Unfallursachen

"In der Regel wird ein Unfall durch mehrere Ursachen ausgelöst, die dann auch vollständig erfasst werden müssen (Ski, S. 61). Eine Beschränkung auf die jeweils überwiegende Ursache ergibt ein verzerrtes Bild, da eine Entscheidung darüber, welche Ursache überwiegt, in vielen Fällen nicht eindeutig getroffen werden kann. Cazamian (zitiert nach Krause, S. 100) unterstellt, dass es sich dabei `nicht so sehr um die wichtigste erscheinende Ursache (handelt), sondern um jene, die ... die einfachste und wirksamste Verhütungsmaßnahme nahe legt.´
Der Zusammenhang der Unfallursachen kann in einer Kausalkette (nach Compes: Kausal-Final-Nexus) oder in einer Kombination, d.h. in gleichzeitigem Vorhandensein, bestehen. Die Wirkungsweise von Unfallursachenketten lässt sich anhand aufrecht gestellter Dominosteine veranschaulichen (Ski, S. 33, vgl. Abb. 8):
Wird der erste Stein zu Fall gebracht, dann fallen auch alle folgenden Dominosteine (Fall 1). Wenn aber ein Stein entfernt wird, werden die folgenden Steine nicht mehr umgestürzt (Fall 2). Damit ist die Ursachenkette

unterbrochen. Das folgende Beispiel stellt eine vereinfachte Unfallursachen-kette dar:
`In einem Steinkohlenbergwerk mit Schlagwettern wird eine Zigarette (verboten!) geraucht und die Kippe achtlos weggeworfen (1). Dadurch entsteht ein Brand (2). Der Brand löst eine Methangasexplosion aus (3). Diese wirbelt Kohlenstaub auf, so dass eine Kohlenstaubexplosion folgt (4). Da die vorgeschriebene Staubsperre (5) fehlt, pflanzt sich die Kohlenstaubexplosion in benachbarte Grubenräume fort, in denen einige Bergarbeiter verletzt werden. Wenn nun beispielsweise kein explosionsfähiges Methan-Luft-Gemisch vorhanden ist, wird die Ursachenkette unterbrochen; der Unfall kann sich nicht mehr ereignen.´ (Ski, S. 33-34)

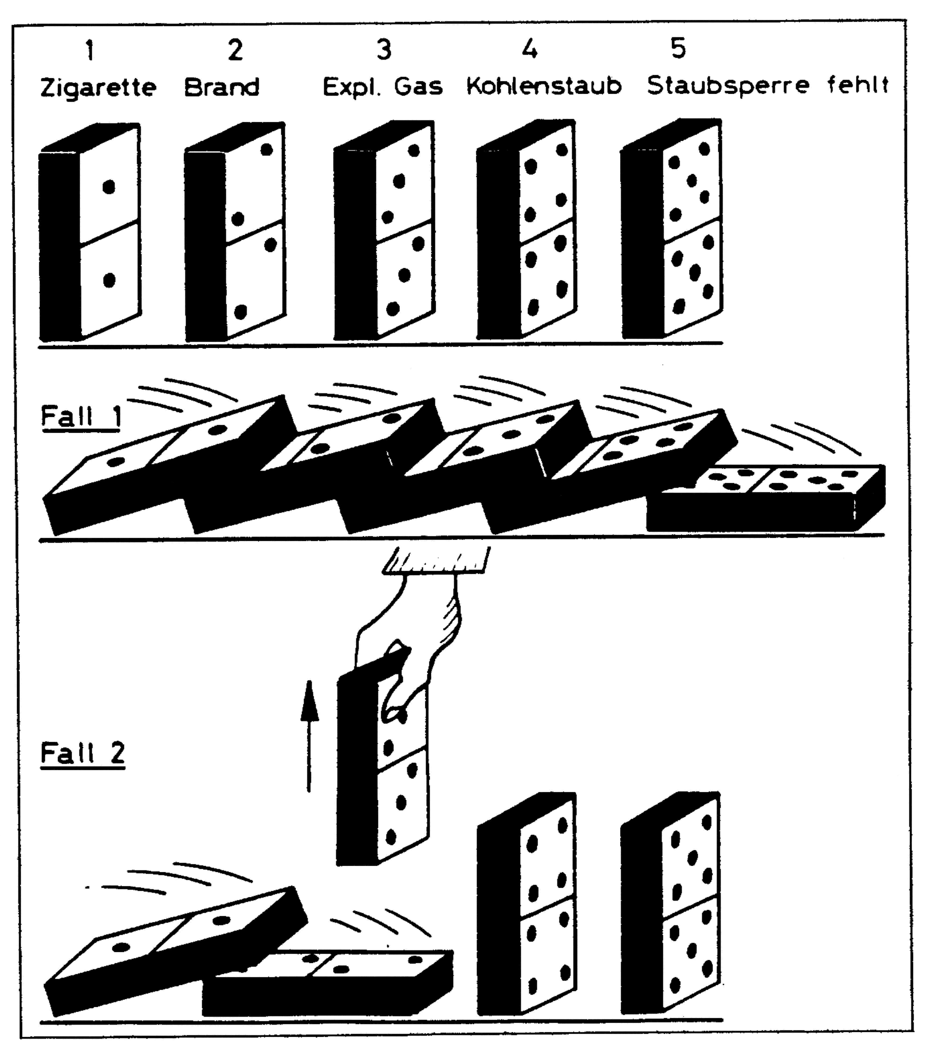


Abb. 8: Unfallursachenketten, veranschaulicht an Dominosteinen (Skiba 1990, S. 33, verändert nach Heinrich, H. W.: Industrial accident prevention - a scientific approach. 4. Aufl. New York : McGraw-Hill, 1959)

Bild 8-1 Unfallursachenkette nach Skiba/Heinrich

Die Unfallursachen können nach unterschiedlichen Kriterien gegliedert werden. Wuppermann (S. 34) stellt einige dieser Unfallursachensystematiken vor. Für die betriebliche Praxis geeignet (Skiba 1990, S. 61) ist eine Untergliederung der Unfallursachen in die Bereiche:

⇒Technik

⇒Organisation

⇒Verhalten

Am stärksten ist der Bereich des Verhaltens in der Unfallstatistik repräsentiert. Dabei darf jedoch nicht außer acht gelassen werden, dass letzten Endes jeder Unfall auf menschliche Unzulänglichkeiten zurückzuführen ist (Wuppermann, S. 32), z.B. bei Konstruktion, Bedienung, Wartung." /Pat, S. 40 -43/

8.4.5 Unfallhergang

Üblicherweise werden für die Beschreibung des Unfallherganges die im Unfallmeldeformular verwendeten Stichworte `Unfallgegenstand´, `Tätigkeit des Betroffenen´ und `Unfallhergang´ als Gliederungskonzept verwendet. Man sollte beachten, dass in der Regel nur Arbeitsunfälle betrachtet werden, d.h. Unfälle, bei denen eine "versicherte Person bei der Ausübung ihrer beruflichen Tätigkeit innerhalb und außerhalb der Arbeitsstätte erleidet." /BMA, S. 4/

Unter dem Stichwort `Unfallgegenstand´ (bzw. unfallauslösender Gegenstand) versteht man einen Gegenstand, "dessen Vorhandensein, Orts- oder Zustandsänderung den vorgesehenen Betriebszustand oder -ablauf gestört und dadurch den Unfall ausgelöst hat." /Hoffm. 1987, S. 70/ Im Sinne der Erfassung für die Statistik der Berufsgenossenschaften ist ein Unfallgegenstand alles, was einen Unfall auslösen kann; z.B. auch ein Lebewesen oder ein Naturereignis.

In vielen Fällen ist es schwer zu entscheiden, ob ein Gegenstand, der auf den Menschen eingewirkt hat und auch den Unfall (mit) verursacht hat, wirklich der Unfallgegenstand ist. Die Ermittlung von unmittelbar den Unfall bewirkenden Gegenständen ist in der Regel einfacher als die Ermittlung und Zuordnung von verursachenden Gegenständen. In den Statistiken der Berufsgenossenschaften wird nur ein einziger unfallauslösender Gegenstand berücksichtigt, was zwangsweise zu Informationsverlusten im Hinblick auf die Unfallursachen führt.

Das nächste Stichwort ist die Tätigkeit des Betroffenen/Verletzten. Darunter versteht man die "auf ein bestimmtes Ziel gerichtete, die körperliche Bewegung ausdrückende Beschäftigung, bei deren Ausführung der Unfall eingetreten ist. Sie ist losgelöst von der Handwerks- oder fachbezogenen Tätigkeit." /BG-S, S. 182/ Als Tätigkeit wird nicht die allgemeine Tätigkeit wie z.B. Reparieren, Fräsen oder Instandhalten angegeben, sondern die konkrete Beschäftigung zum Zeitpunkt des Unfalls; also beispielsweise Heben (eines Ersatzteiles), Hantieren

mit einer Handschleifmaschine oder Befestigen des Werkstückes mittels der Spannvorrichtung.
Das letzte der drei Stichworte ist Unfallvorgang. Unter diesem Stichwort wird die Art des Zusammenwirkens von Mensch und Gegenstand während des Unfallereignisses beschrieben. In den Statistiken der Berufsgenossenschaften wird dieses Stichwort aufgespaltet in die Unterpunkte `Bewegung des unfallauslösenden Gegenstandes´ und `Bewegung des Verletzten´.

8.4.6 Unfallfolgen

"In der Literatur wird als Unfallfolge vor allem der Körperschaden berücksichtigt, auch wenn in grundsätzlichen Überlegungen gefordert wird, zusätzlich Unfälle mit Sachschaden und möglichst auch Betriebsstörungen zu erfassen und zu untersuchen. Zur Charakterisierung eines Körperschadens wird der verletzte Körperteil, die Art der Verletzung und die Unfallschwere angegeben.

Verletzter Körperteil

Der verletzte Körperteil kann als Unfallfolgemerkmal `zusammen mit anderen Merkmalen wesentlich zur Analyse beitragen. Auch lässt sich an Hand der verletzten Körperteile feststellen, inwieweit die Einführung von persönlicher Schutzausrüstung Erfolg haben kann oder bereits hatte´ (Skiba 1990, S. 65). Anzumerken ist dazu, dass amtliche Statistiken, die sich auf Angaben in der Unfallanzeige stützen, für jeden Unfall nur einen verletzten Körperteil berücksichtigen. Bei Verletzung mehrerer Körperteile wird der am schwersten betroffene bzw. der gesamte Mensch (z.B. bei großflächigen Verbrennungen oder Verätzungen) als verletzter Körperteil verschlüsselt (BG-Schlüssel 1983a, S. 21). ...

Verletzungsart

In den Statistiken der Berufsgenossenschaften werden zehn verschiedene Verletzungsarten unterschieden (BG-Schlüssel 1983a, S. 27):

⇒Commotio (alle Formen der Erschütterung),

⇒Contusio (alle Formen der Prellung, Quetschung u.ä.),

⇒Distorsion (alle Formen der Verstauchung),

⇒Luxation (alle Formen der Verrenkung),

⇒Zerreißung (alle Formen offener und geschlossener Zerreißungen von Gewebe und Organen),

⇒Geschlossener Knochenbruch,

⇒offener Knochenbruch,

⇒Verbrennung, Erfrierung, Verbrühung, Verätzung, Verstrahlung,

⇒Infektion, Vergiftung (außer Berufskrankheiten und

⇒sonstige oder nicht näher bezeichnete Verletzungsart.

Unfallschwere

In Anlehnung an die Statistiken der gesetzlichen Unfallsversicherungsträger ist häufig folgende Einteilung der Unfallschwere anzutreffen (Schulz 1973, S. 57; Skiba 1990, S. 65):

1. Unfall ohne Arbeitsausfall
2. Nicht anzeigepflichtiger Unfall
3. Anzeigepflichtiger Unfall
4. Entschädigungspflichtiger Unfall
5. Tödlicher Unfall

Ein Unfall ist anzeigepflichtig, `wenn eine versicherte Person durch einen Unfall getötet oder so verletzt wird, dass sie stirbt oder für mehr als drei Tage völlig oder teilweise arbeitsunfähig ist´ (BMA 1990, S. 4).

Als erstmals entschädigt gilt ein Unfall, `wenn wegen der Folgen des Unfalls ... im Berichtsjahr erstmals eine Rente, eine Abfindung oder ein Sterbegeld gezahlt worden ist´ (BMA 1990. S. 4).

Dieses Einteilungsprinzip ist für Verwaltungszwecke bestimmt und geeignet (Schulz 1973, S. 58). Für die Verwendung in der Unfallforschung erweist sich als nachteilig, dass die einzelnen Schwerearten nicht eindeutig voneinander getrennt sind, da z.B. erstmals entschädigte und tödliche Unfälle gleichzeitig anzeigepflichtige Unfälle sind. Außerdem ist zu berücksichtigen, dass zwischen der Anzeige und der Erstentschädigung des Unfalls immer ein längerer Zeitraum liegt. Dies kann auch für den tödlichen Unfall zutreffen.

Als geeigneter Maßstab für die Unfallschwere ist aus mathematisch-statistischer Sicht die Anzahl der Ausfalltage anzusehen (Schulz 1973, S. 62). Der Vorteil liegt darin, dass die Zahl der ausgefallenen Arbeitstage messbar ist. Dadurch können die Unfälle beliebig in Klassen eingeteilt werden, was im Extremfall zu einer Klassenbreite von einem Tag führen kann. In der Praxis ist die Verwendung der Zahl der Ausfalltage als Maßstab der Unfallschwere nicht unproblematisch. So können Untersuchungen erst dann durchgeführt werden, wenn die Verletzten wieder arbeitsfähig sind und somit die Anzahl der Ausfalltage feststeht. Ferner können gleichartige Verletzungen je nach körperlicher Konstitution des Verletzten, ärztlicher Betreuung, Einschätzung des behandelnden Arztes hinsichtlich der Arbeitsfähigkeit, Art der Tätigkeit des Verletzten usw. zu verschieden langen Ausfallzeiten führen. Bei einem tödlichen Unfall wird für die Ausfallzeit ein fester Wert von 6000 bzw. 7500 Tagen eingesetzt (Schulz 1973, S. 65). Ein weiteres Problem ist die Bewertung von

Unfällen mit Verlust bzw. ständiger Minderung der Erwerbsfähigkeit. Trotz der genannten Probleme ist die Anzahl der Ausfalltage der geeignetste der für die Unfallschwere verwendbaren Maßstäbe, da damit feinere Abstufungen und aussagekräftigere Ergebnisse erzielt werden können (Schulz 1973, S. 67)

Sachschaden

In den Unfallstatistiken der Berufsgenossenschaften tritt der Sachschaden nicht in Erscheinung. Der Grund dafür ist, dass gegen die Unfallversicherungsträger nur wegen eines Personenschadens ein Anspruch erhoben werden kann. \`Für Sachschäden haftet allein der Schädiger nach zivilrechtlichen Vorschriften, niemals die Berufsgenossenschaft´ (Hoffmann 1990, S. 50). Für die Unfallforschung sind aber auch solche Fälle einzubeziehen, durch die lediglich ein Sachschaden entsteht, da unter geringfügig geänderten Bedingungen die Wahrscheinlichkeit für einen Personenschaden zunehmen kann. ...
Geht man bei der Beurteilung eines Sachschadens ähnlich vor wie beim Personenschaden, erscheint eine Gliederung in

⇒beschädigter Gegenstand,

⇒Art der Beschädigung und

⇒Schwere der Beschädigung
angebracht. Unter diesen Voraussetzungen lassen sich folgende Überlegungen anstellen:
Für die Gegenstände lässt sich eine Liste aufstellen, die alles das enthält, was bei einem Unfall mit (Personen- und) Sachschaden beschädigt oder zerstört werden kann. Diese Liste kann sehr umfangreich und dadurch unübersichtlich werden, da nicht von vornherein erkennbar ist, inwieweit die Aufnahme einzelner Bestandteile von Geräten, Apparaten, Maschinen oder Anlagen in diese Liste geeignet ist.
Eine solche Liste von Gegenständen an sich ist für die Unfallforschung und die Unfallverhütung von geringem Wert. Diese Gegenstände müssen zusätzlich ihrer Funktion während des Unfalls zugeordnet werden können.
Für die Einteilung der Gegenstände z.B. in der Produktion sind folgende Kriterien denkbar:

⇒Gegenstände, die der Bearbeitung dienen: Werkzeug, Gerät, Maschine(-nteil) usw.

⇒Gegenstände, die bearbeitet werden oder wurden: Halbzeug, Fertigprodukt usw.

⇒Gegenstände, die mittelbar mit der Bearbeitung in Zusammenhang stehen: Schmiermittel, Hilfsstoff usw.

⇒Transportmittel: Schubkarre, Förderband, Gabelstapler, Kran, Rutsche usw.

⇒Gebäude (-teile): Außenwand, tragende und nicht tragende Innenwand, Mauerstein, Gipskartonplatte usw.

⇒Gegenstände, die zur Raumausstattung gehören: Beleuchtung, Heizung usw.

⇒sonstige Gegenstände, insbesondere solche, die an der Unfallstelle fehl am Platz sind: eine `vergessene´ Leiter, ein mitgebrachter Tischventilator usw.

Vorstellbar ist, dass für einzelne Bereiche derartige Listen von ausreichendem Umfang und ausreichender Qualität mit vertretbarem Aufwand erstellt werden können. Zu berücksichtigen ist dabei, dass ein Gegenstand beim Sachschaden sowohl als unfallauslösender (`Täter´) als auch als beschädigter Gegenstand (`Opfer´) in Betracht zu ziehen ist.
... die Art der Beschädigung lässt sich nicht ohne weiteres für alle Gegenstände verallgemeinern, da Aufbau und Form der Gegenstände sehr unterschiedlich sind.” /Pat, S. 51 - 55/ Ebenso muss man entscheiden, ob man den Gegenstand an sich betrachtet oder als Teil eines anderen Gegenstandes (z.B. Maschine). Wenn man den Gegenstand als Teil eines Anderen sieht, muss man bestimmen, ob dieser Teil für die Maschine wichtig ist oder unwesentlich.
Die Schadensschwere eines Sachschadens wird in der Regel in Geldwert festgestellt. Dies wird aus versicherungstechnischen Gründen so gehandhabt. Es existieren einige andere Vorschläge, die aber nur in Einzelfällen angewendet werden. /vgl. hierzu Fra, S. 80 ff. und S. 128 ff./

8.5 Ein staatlich gefördertes Programmbeispiel

Eines der ersten Programme in diesem Arbeitsfeld war `RASI´ (= Rechnergestützte Arbeitssicherheit). Es wurde vom Hoesch-Konzern entwickelt. Zielsetzung war, den Arbeitsschutz weiter zu verbessern. Bei Hoesch vertrat man die Auffassung, dass mit konventionellen Methoden keine weitere Verbesserung des erreichten hohen Sicherheitsstandards möglich sei. Man beantragte daher eine finanzielle Förderung durch das Bundesministerium für Arbeit und Sozialordnung für die Entwicklung und den Aufbau einer EDV-gestützten Unfalldatenverarbeitung, -verwaltung und – analysemöglichkeit. Diesem Antrag wurde stattgegeben und zum 1. 9. 1984 wurde mit dem Projekt begonnen.
“Wegen der Neuartigkeit der Aufgabenstellung und dem damit verbundenen Erfolgsrisiko wurde nicht ein konzernweiter Rechnereinsatz in Erwägung gezogen, sondern aufgrund ihrer repräsentativen Anforderungsstruktur (u.a. Unternehmensgröße, Produktpalette, Organisationsform) die Konzerngesellschaft Hoesch Hohenlimburg AG für dieses Vorhaben ausgewählt. Hierfür

sprach auch die bei der Hoesch Hohenlimburg AG lückenlos vorhandene Erfassung aller Unfallereignisse als Voraussetzung für eine umfassende rechnergestützte Bearbeitung des Unfallgeschehens." /RASI/

Es wurden die betrieblichen Führungskräfte sowie die betroffenen Mitarbeiter als auch der Betriebsrat stets informiert und zur Mitarbeit gewonnen. Daher fand das Projekt eine gute Akzeptanz. Die notwendige Systemanalyse wurde durchgeführt und darauf aufbauend wurde ein für damalige Zeiten moderner PC beschafft. Die benötigten Programmteile wurden in der Programmiersprache Cobol von der Zentralen Datenverarbeitung geschrieben, da zu dieser Zeit keine ausgereiften Datenbanksysteme angeboten wurden, die auf PCs lauffähig waren. Cobol wurde auch daher gewählt, da man in der Zentralen Datenverarbeitung über langjährige Erfahrungen mit Cobol verfügte. Da Nicht-EDV-Fachleute mit diesem Programm arbeiten sollten wurde nach (für diese Zeit) modernsten software-ergonomischen Gesichtspunkten programmiert. Menütechnik wurde benutzt; viel Wert wurde auf eine gute Benutzerführung und eindeutige Maskenausführung gelegt. In der Einführungsphase arbeiteten die Abteilungen Arbeitssicherheit und zentrale Datenverarbeitung eng zusammen, um Fehler zu beseitigen und die Software zu optimieren.

"In Anlehnung an die bestehende Organisation der Hauptabteilung `Arbeitssicherheit´ und unter Berücksichtigung, dass bei der gewählten Anlagenkonfiguration zur Zeit noch keine Mehrplatzfähigkeit über eine größere Entfernung gegeben ist, musste die Eingabe von Daten auf die beiden Sachbearbeiterinnen aus dem Verwaltungsbereich übertragen werden. Dies hatte zur Konsequenz, nach der Eingabe von Unfallmeldenummer, Name und Vorname des Verletzten sowie Stammnummer für jeden Unfall einen Eingabebeleg auszudrucken, den die einzelne Sicherheitsfachkraft für ihren Zuständigkeitsbereich mit der Erstellung der Unfallanalyse und der Festlegung von Unfallursachen zu bearbeiten hat, um danach die Eingabe der Daten zu veranlassen.

Als Arbeitsergebnisse können Listen mit unterschiedlichen Informationsgehalten über einen Drucker abgerufen werden. Dabei sind zwei Arten von Listenausdrucken zu unterscheiden. In Abhängigkeit vom Informationsgehalt werden zum einen Listen für die betrieblichen Führungskräfte und Betriebsräte und zum anderen Listen als interne Arbeitsunterlagen für die Sicherheitsfachkräfte erstellt.

Die Mitarbeiterinnen und Mitarbeiter der Hauptabteilung `Arbeitsicherheit´ sind zum Schutz personenbezogener Daten verpflichtet. Diese Verpflichtung wurde bei der Erstellung der Listen für die betrieblichen Führungskräfte und Betriebsräte beachtet. Durch interne Regelungen und technische Maßnahmen ist eine missbräuchliche Benutzung des Rechnersystems ausgeschlossen." /RASI/

8.6 *Anforderungen an ein Unfalldatenerfassungs- und -bearbeitungsprogramm*

Wie schon im vorhergehenden Kapitel erwähnt, ist bei der Beschaffung oder Erstellung eines solchen Programms auf manche Dinge zu achten, die man vorher entweder als selbstverständlich und gegeben oder als unwichtig oder unnötig erachtet hat. Der allgemeine Teil (Kpt. 8.6.1) ist mit dem Text zu Gefahrstoffprogrammen identisch – abgesehen von den Beispielen. Er wird trotzdem noch mal abgedruckt, um Zurückblättern zu vermeiden, falls man mit Gefahrstoffprogrammen nichts zu tun hat(te).

Auch hier ist es so, dass manches Programm eine bestimmte Hardware und/oder Software (Betriebssystem, Benutzeroberfläche usw.) benötigt. Oft werden bestimmte EDV-Kenntnisse vom Entwickler und später vom Vertreiber solcher Programme vorausgesetzt. Insbesondere bei den Unfallanalyseprogrammen sollte man über etwas EDV-Verständnis verfügen, wenn man diese Programme richtig ausnützen will. Bei den Planungen der Kosten der Programmbeschaffung wird auch bei der Beschaffung dieser Programme gern vergessen, dass Kosten für Schulung, Programmpflege, Hot-Line-Service, technische Unterstützung bei Installation und Einführung anfallen. Dazu kommt, dass in der Regel der Erstarbeitsaufwand vollkommen falsch eingeschätzt wird, oft viel zu niedrig angesetzt ist. Man muss sich mit den allgemeingültigen Regeln zu Softwareergonomie und Datenschutz/-sicherheit vertraut machen. So werden jetzt noch in - wenn auch wenigen - Programmen elementare software-ergonomische Regeln nicht beachtet bzw. nicht angewendet und dadurch die Arbeit damit unnötig erschwert. Da personenbezogene Daten verarbeitet werden, müssen die Datenschutzvorschriften beachtet werden. Ein Paßwortschutz sollte vorhanden sein und die in der Datenbank abgelegten Daten sollten verschlüsselt sein, so dass sie nicht unter Umgehung der Datenbank gelesen oder manipuliert werden können.

8.6.1 Allgemeine Anforderungen

Nach DIN sollte ein Programm (ganz allgemein gültig) folgende Grundsätze erfüllen. Es sollte

1. aufgabenangemessen,
2. selbstbeschreibungsfähig,
3. steuerbar,
4. erwartungskonform und
5. fehlerrobust sein.

Aufgabenangemessen bedeutet, dass der Anwender bei der Erfüllung seiner Aufgaben vom Programm unterstützt wird, ohne zusätzlich durch Eigenschaften des Programms belastet zu werden. D.h. also, dass solch ein Programm die Arbeit erleichtern und nicht erschweren soll.

Will man z.B. neue Unfalldaten eingeben, sollten übersichtliche und geordnete Eingabemasken da sein. Der Datenblattaufbau sollte immer gleich sein. Sinnvolle Vorgaben, die einfach überschrieben werden können, unterstützen die Eingabe zusätzlich.
Wenn (z.B. Unfall-) Daten ausgegeben werden, sollten sie formatiert sein, dass der Anwender sich leicht zurechtfindet. Alle wichtigen Daten (des Unfalles) sollten leicht aufnehmbar sein.

Selbstbeschreibungsfähig ist ein Programm dann, wenn es dem Anwender direkte Informationen über seinen Umfang, seinen Aufbau, seine Aufgaben und seine Steuerbarkeit gibt. Das bedeutet für solch ein Programm: man soll sehen, was das Programm alles leistet bzw. was es für Module (Unfalldatenerfassung, Unfallanzeige erstellen, Unfallanalyse usw.) anbietet, wo man sich befindet (Unfalldaten eingeben, Unfallanalyse durchführen, Unfallanzeige ausdrucken ...), wo man wie hingelangt (z.B. von Unfalldateneingabe zu Unfallanzeige ausdrucken). Die Dialogschritte haben unmittelbar verständlich zu sein.
Ein Hilfemodul soll dem Anwender auf Verlangen Informationen zur Handhabung, zu bestimmten Feldern oder Meldungen in einer ihm verständlichen Ausdrucksweise geben. Für die Dateneingabe eines noch nicht erfassten Unfalles in einem Unfallerfassungsdatenblatt bedeutet dies, dass entweder die Titel der Eingabefelder so gewählt sind, dass man weiß, was man einzugeben hat oder falls dies nicht möglich ist, für die Felder ein Erklärung angeboten wird, welche die notwendigen Informationen zur Eingabe beinhaltet.

Ein Programm wird als *steuerbar* bezeichnet, wenn es dem Anwender ermöglicht, ohne starre Menüabläufe von einem Teil des Programms zu einem anderen zu gelangen. Beispielsweise sollte man von Eingabe von Unfalldaten direkt zu Ausdrucken oder Erstellen einer Unfallanzeige wechseln können, ohne zum Ausgangsmenü zurückzukehren. Es ist auch wichtig, dass man einen Arbeitsschritt unterbrechen oder gar abbrechen kann. Der letzte Arbeitsschritt sollte widerrufbar sein. Verarbeitungsprozesse, die eine größere Tragweite haben, sollten erst nach einer Bestätigung ausgelöst werden. Es ist natürlich irgendwo nervend, wenn man vom Programm irgendwas besonderes verlangt, dies dauernd noch mal extra zu bestätigen. Spätestens aber, wenn man ein Unfalldatenblatt aus Versehen gelöscht hat, und dies wieder frisch eingeben muss, lernt man die beiden letztgenannten Forderungen zu schätzen.
Eine Forderung ist (leider) immer noch bei vielen Programmen nicht realisiert: Bei Unterbrechungen und Störungen durch einen Systemausfall sollte der Anwender seine Arbeit beim letztdurchgeführten Dialogschritt wieder aufnehmen können. Eine Realisierung dieser Forderung würde bedeuten, dass nach jedem Arbeitsschritt gesichert werden müsste. Darunter würde natürlich die Schnelligkeit des Programms leiden.

Ein Programm verhält sich *erwartungskonform*, wenn

⇒das Programm sich so verhält, wie im Handbuch beschrieben ist,

⇒das Dialogverhalten und die Dialogführung einheitlich ist,

⇒(gleiche) Aktionen des Anwenders sofort zu (gleichen) Reaktionen des Programms führen und

⇒Abweichungen von den ersten drei Punkten erklärt werden.

Diese Erwartungskonformität ist der Hauptgrund, warum ein Unfalldatenblatt, eine Unfallanalysemaske oder auch eine Unfallanzeige immer gleich aufgebaut sein sollen.

Die Eigenschaft `*fehlerrobust*´ ist mittlerweile Standard. Man bringt durch falsche Eingaben fast keine Programme mehr zum Absturz. Ebenso die Informationen über Art und Ort des Fehlers sind in der Regel ausreichend. Nur die Hinweise zur Fehlerbehebung sind in manchen Programmen etwas dürftig geraten.

8.6.2 Aufgabenspezifische Anforderungen

Die bisher beschriebenen Anforderungen gelten ganz generell wie ein Vergleich mit den im vorhergehenden Kapitel beschriebenen Gefahrstoffprogrammen zeigt. Die im folgenden beschriebenen Anforderungen sind speziell auf Unfallerfasungs- und -bearbeitungsprogramme bezogen.

Der Unfalldatenerfassungsteil muss so komfortabel wie möglich sein und eine schnelle Eingabe der Daten gestatten. Es muss möglich sein, die Daten mindestens so schnell einzugeben wie ein sauberes Ausfüllen des Unfall-meldeformulars (Unfallanzeige) von Hand dauert. Es sollten zumindest alle Daten abgefragt werden, die auch beim manuellen Ausfüllen der Unfallanzeige benötigt werden. Für die Unfallursachenerforschung ist es wünschenswert, wenn mehr Informationen zum Unfallereignis abgefragt werden als es die Unfallanzeige vorsieht. Es ist oft von Vorteil, einen schon ausgefüllten Datensatz benutzen zu können. In so einem Fall sollte eine Sicherung da sein, dass man den ursprünglichen Datensatz nicht löscht, indem man unter dem alten Namen abspeichert. Wichtig ist, wie schon im vorhergehenden Abschnitt erklärt, dass die Datenblätter/-sätze alle gleich aufgebaut sind. Wenn man in der Datenbank etwas sucht, sollte es möglich sein, alle Unterpunkte als Suchkriterium zu verwenden. Ebenso sollten die Daten nach allen Unter-punkten sortierbar sein. Die Unfallanzeige muss direkt ausdruckbar sein und sollte dem BG-Formular auch optisch entsprechen.

Der statistische Teil ist einerseits für das Berichtswesen interessant, andererseits soll dieser Programmteil bei der Unfallursachenforschung als Hilfsmittel verwendet werden. Für das Berichtswesen ist es notwendig, dass entweder graphische Darstellungsmöglichkeiten angeboten werden oder eine Schnittstelle zu entsprechenden Programmen vorhanden ist. Für die Unfallursachen-

forschung ist es wünschenswert, dass mehrere Unterpunkte miteinander verknüpft und die einzelnen Unfälle dementsprechend sortiert werden können. Folgende spezielle Anforderungen sollte ein Unfalldatenerfassungs- und -bearbeitungsprogramm also erfüllen:

⇒Immer gleicher Datenblattaufbau

⇒Zumindest die Unterpunkte abfragen, die zum Drucken der Unfallanzeige nötig sind

⇒Auswahlmenüs, wo dies möglich ist

⇒Suchmöglichkeit nach allen Unterpunkten

⇒Gute Ergänzungsmöglichkeit

⇒Automatische Sicherung

⇒Sicherung gegen versehentliches Überschreiben

⇒Ausdrucken der Unfallanzeige `per Knopfdruck´

⇒Graphische Darstellungsmöglichkeiten oder

⇒Schnittstelle zu Graphikprogrammen

⇒Gute Verknüpfungsmöglichkeiten

Literatur

Ale Aleanakian, Gabriel / Kühnau, Walther
Datensicherung bei Personalcomputern
Vogel-Buchverlag Würzburg 1986

Bam Bamberg, Günter / Baur, Franz
Statistik
R. Oldenbourg München 1980

Bar Bartsch, Michael
Das DIN Deutsches Institut für Normung e.V. als marktbeherrschende Unternehmung i.S.v. § 22 GWB
Diss. Uni Münster 1987

Bas Büroarbeitsplätze sicher und gesund
Bundesarbeitsgemeinschaft für Arbeitssicherheit (BASI)
Düsseldorf, Juli 1992

Bec Becker, M. et al
EDV-Wissen für Anwender; ein Handbuch für die Praxis
Verlag Industrielle Organisation München 1983 2. Auflage

Beu Beuth Verlag GmbH 10772 Berlin
PERINORM – Verzeichnis der Normen

BG-S Hauptverband der gewerblichen Berufsgenossenschaften
Schlüsselverzeichnis zur Unfallanzeige
Lose Blatt Ausgabe, Stand 1983

BMA Bundesminister für Arbeit und Sozialordnung
Arbeitssicherheit 1990 - Unfallverhütungsbericht
Bonn 1990

Chris Christoph, Uwe
Der Bildschirmarbeitsplatz
Dr. Curt Haefner Verlag GmbH Heidelberg 1992

CHV Carl Heymannsverlag KG, Luxemburger Straße 449, 50939 Köln
ÜA-Verzeichnis (Trxxx, ASR, D, KTA)
Verzeichnis der VBG-Vorschriften
Verzeichnis der ZH 1-Schriften

Com-BW Compes, P.C. / Franke, U. / Schulze-Wege / Vieweg, S.
BW-Studie
nicht veröffentlicht

Com-EWI Compes, Peter Constantin
EWI-Studie
nicht veröffentlicht

CSD Lehmann, Thomas
Chemikalien-Sicherheits-Datenbank Hinweise
www.chemie.fu-berlin.de/user/Lehmann/chemsaf2.htm

DFG DFG
Maximale Arbeitsplatzkonzentration und Biologische Arbeitsstofftoleranzwerte
VCH Verlagsgesellschaft mbH Weinheim 1987

Dic Dickschus, Arthur
Rund um den PC
Markt und Technik Verlag AG München 1991

Dre Drechsel, Manfred
Praxistipps zur Virenabwehr
in Networks & Communication Neue Mediengesellschaft Ulm 6/95

Fra Franke, Uwe
Das Phänomen `Schaden´ sicherheitstechnisch
GfS Wuppertal 1993

Fit FitzGerald, Nick
Computer. Virus - Frequently Asked Questions
gefunden in Newsgroups: comp. virus; last updated Oktober 1995

GDD Gesellschaft für Datenschutz und Datensicherung e.V.
Datenschutz und Datensicherung im Unternehmen
Bonn 1992
GDD Geschäftsstelle: Irmintrudisstr. 1a, 53111 Bonn

Ger Gerken, Wolfgang
Systemanalyse - Entwurf und Analyse von DV-Anwendersystemen
Addison-Wesley Bonn New York 1988

GES GESTIS Stoffdatenbank
http://www.hvbg.de/d/bia/fac/zesp/zesp.html
Berufsgenossenschaftliches Institut für Arbeitssicherheit St. Augustin

Gra Graßl, Michael / Sinks, Volker
Arbeitsicherheit und Unfallverhütung im öffentlichen Dienst
2. Auflage, ecomed Verlagsgesellschaft Landsberg, München 1989

Gro	Grochla, Erwin Datenschutz im Betrieb Vieweg-Verlag Braunschweig Wiesbaden 1982
Gru	Gruber, A., Boes, W Datenverarbeitung in Verwaltung und Wirtschaft Band 2: Planung und Organisation Walhalla und Praetoria Verlag Regensburg 1983
GUB	WAUplus - Arbeitsschutzsoftware http://wauplus.ckc.de GUB Braunschweig
Hag	Hagen, Willi / Pauwels, Armin / Suttrop, Werner / Wichert, Oskar Rechnergestützte Arbeitssicherheit Schriftenreihe der BAU - Forschung - Fb 483 NW-Verlag Bremerhaven 1986
Har1	Hartung, Peter Was bieten EDV-Systeme im Arbeitsschutz in die BG, April 1991, S. 198 ff.
Har2	Hartung, Peter Auswahl von computerunterstützten Arbeitsschutz-Systemen Amtliche Mitteilung der Bundesanstalt für Arbeitsschutz Dortmund 1993
HBV	Gewerkschaft HBV Hessen Geltungsbereich der Bildschirmarbeitsverordnung - Autorin: Regine Rundnagel Pausen bei Bildschirmarbeit – Autorin: Ulla Wittig-Goetz Gestaltungsanforderungen für die Bildschirmarbeit - Autorin: Regine Rundnagel http://www.sozialnetz-hessen.de/ergo-online
Hei	Heiler, Siegfried/ Rinne, Horst Einführung in die Statistik A. Hain Meisenheim 1971
HMW	Hessisches Ministerium für Frauen, Arbeit und Sozialordnung Gefahrstoffdatenbank der Länder Wiesbaden 1994
Hof	Hoffmann, Friedrich Computergestützte Informationssysteme Oldenbourg Verlag München Wien 1984

Hoff	Hoffmann, Burkhard Unfallanalyse 1985 Hauptverband d. gew. Berufsgenossenschaften St. Augustin 1987
Hoff	Hoffmann, Burkhard Arbeitsschutz und Unfallstatistik 1988 Hauptverband d. gew. Berufsgenossenschaften St. Augustin 1990
ICS	Stang, David J. ICSA´s Computer Virus Handbook Second Edition April 1992
Imp	impec-Katalog Katalog der impec Computervertriebs GmbH Tübingen 1994
Jab	Jaburek, Walter Risiken elektronischer Datenübermittlung im ... Reihe Informatik, Band 73 BI Wissenschaftsverlag Mannheim/Wien/Zürich 1990
JMV	BETRAN - Arbeitsschutzsoftware http://www.jedermann.de/angebot/betran.html Jedermann Verlag Heidelberg
Kir	Kirste, Burkhard Das Internet und die Internetdienste (Vortrag) 2. Workshop im Projekt "Endnutzerförderung Chemiedatenbanken" Frankfurt am Main, 19. Mai 1995
Kloe	Kloepfer, Michael Datenschutz als Grundrecht Athenäum Verlag Königstein 1980
Krause	Krause, Horst Erfassung, Auswertung und Darstellung des Unfallgeschehens In: Krause/Pillat/Zander, Arbeitssicherheit, Gruppe 4, S. 45 - 132 R. Haufe Freiburg Stand 1991
Kru	Krueger, Helmut Arbeiten mit dem Bildschirm - aber richtig Bayrisches Ministerium für Arbeit und Sozialordnung 9. Auflage München 1989
Lac	Lackmann-Gubela, Martin Von der Bedrohungslage zum Sicherheitskonzept in IT-Sicherheit am Arbeitsplatz, S. 5 ff. Informationsschrift zum internationalen SiTech-Kongreß, Berlin 1993

Lan
Langemeyer, Paul
Viren und kein Ende
in IT-Sicherheit am Arbeitsplatz, S. 43 ff.
Informationsschrift zum internationalen SiTech-Kongreß, Berlin 1993

Leu
Leuwico Ergo
Willkommen bei Leuwico
http://www.ckunst.de/leuwico/ergo/ergo.html

Lin
Lindemann, Peter
Leitfaden Datenschutz und Datensicherheit für Klein- und Mittelbetriebe
AWV Fachinformation Eschborn 1980

LNW
Landesumweltamt Nordrhein-Westfalen
Das Informations- und Kommunikationssystem für gefährliche und umweltrelevante Stoffe
Essen 1994

Men
Mensch und Technik
Auswirkungen computerisierter Arbeit auf Menschen im Hinblick auf Vorbeugung von Krankheit und Erhaltung von Gesundheit - Computerarbeit und Gesundheit
Ministerium für Arbeit, Gesundheit, Familie und Sozialordnung von Baden-Württemberg
Institut für Mensch und Arbeitswelt, Prof. Affemann, Baden-Baden
Stuttgart, November 1989

Nie
Niedecker, Klaus
Systemanalyse und Risikokontrollmaßnahmen zur Gefährdungsvermeidung in Gefahrstofflagern
Diplomarbeit Allgemeine Sicherheitstechnik 1995

Pat
Patrzek, Georg
Entwurf eines Programm-Moduls zur Unfalldaten-Bearbeitung
Diplomarbeit Allgemeine Sicherheitstechnik 1993

Pilz
Pilz, Robert / Thiele, Brun (Bearb.)
Arbeitssicherheit ist eine Leistung: Leitfaden für die Unfallverhütung im Betrieb
E. Schmidt Berlin 1970

Poh
Pohlschröder
Mehr Ideen pro m^2 Nr. 1; Alles über die neuen EU-Richtlinien für Bildschirmarbeitsplätze
Pohlschröder GmbH & CoKG, Dortmund 1994

Sac Sachs, Lothar
Statistische Methoden; ein Soforthelfer
Springer Berlin 1970

Sam Samlowski, Wolfgang
Perspektiven wissensbasierter Systeme im Arbeitsschutz
in EDV im Arbeitsschutz - Vorträge der Informationstagung am 22. und 23. April 1991 in Dortmund, S. 41 ff.
Schriftenreihe der BAU - Tagungsbericht - Tb 55
NW-Verlag Bremerhaven 1991

Sas VDSI-Arbeitskreis Nordbayern
EDV im Arbeits- und Umweltschutz
Wiesbaden 1991

Sche1 Scheil, Michael
Tätigkeitsanalyse des Sicherheitsingenieurs (Teil 1)
in sicher ist sicher, 4.96, S. 172 ff.

Sche2 Scheil, Michael
Tätigkeitsanalyse des Sicherheitsingenieurs (Teil 2)
in sicher ist sicher, 6.96, S. 294 ff.

Schu Schubert, Klaus
EDV im Arbeitsschutz - eine Bestandsaufnahme von Praxislösungen und Entwicklungen
in EDV im Arbeitsschutz - Vorträge der Informationstagung am 22. und 23. April 1991 in Dortmund, S. 41 ff.
Schriftenreihe der BAU - Tagungsbericht - Tb 55
NW-Verlag Bremerhaven 1991

Schue Schürhoff, Stefan
Evaluation von Bildschirmarbeitsplätzen
Diplomarbeit Allgemeine Sicherheitstechnik 1994

Schulz Schulz, Udo
Statistik als Grundlage der Unfallforschung
Methoden, Probleme und Praxis der Arbeitsunfallstatistik
Hauptverband der gewerblichen Berufsgenossenschaften Bonn 1973

sis o.A.
EDV-Sonderschau übertraf Erwartungen
in sicher ist sicher, 2.87, 38. Jahrgang Nr. 2, S. 79 f.

Ski Skiba, Reinald
Taschenbuch Arbeitssicherheit, 6. Auflage
E. Schmidt Bielefeld 1990

Sla Slade, Robert
Robert Slade´s Guide to Computer Viruses
Second Edition Springer New York, Berlin, Heidelberg 1996/1995

Ste Stein, G / Kunze, G
Arbeitssicherheit - Pflichten der Versicherten und der Betriebsräte
Verlag Technik & Information Bochum 1991

Tro Troitsch, Michael
PC-Vernetzung
Der sichere Weg zum individuellen LAN
Franzis Verlag München 1988

Utt Utter, Georg
Erarbeitung und Beschreibung der Grundlagen für die Planung und Konzeption eines Systems zur rechnerunterstützten Unfalldatenaufnahme und -verarbeitung ...
Diplomarbeit am Fachgebiet Allgemeine Sicherheitstechnik 1989

Wer Werner, E.; Bau, M.; Frielingsdorf, R.; Romahn, H..; Romahn, R.
Arbeitszeit und Unfallgeschehen
Schriftenreihe der BAU, Forschungsbericht 216
Wirtschaftsverlag NW Bremerhaven 1979

Wic Wichelhaus, Klaus
Dokumentation und Erstellung eines Programm-Moduls zur Unfalldaten-Erfassung
Studienarbeit am Fachgebiet Allgemeine Sicherheitstechnik 1990

Woh Wohlgemut, Hans
Datenschutz für Arbeitnehmer
Luchterhand Neuwied 1988

Wun Wunenburger, Heidi
Marktuntersuchung zur Ermittlung des EDV-Angebotes in der Arbeitssicherheit
Studienarbeit am Fachgebiet Allgemeine Sicherheitstechnik 1995

Wup Wuppermann, Carl L.
Analyse des Unfallgeschehens im Betrieb
Wilfer Spardorf 1985

Anhang

Anhang 2-6

Interessante Web-Adressen

Es handelt sich um eine Auswahl von Web-Adressen, die in der Hauptsache den Inhalt des Buches widerspiegeln und ergänzen. Einige Seiten sind bei weitem nicht mehr so großzügig wie früher, da viele der gegebenen Informationen kommerziell ausgenutzt wurden. Andere Seiten sind ausführlicher geworden. Es werden Web-Adresse, Inhaltangabe bzw. der inhaltliche Schwerpunkt und Anmerkungen angegeben. Der Stand ist Frühjahr 2000.

Hochschulen, Forschungsinstitutionen

Fachhochschule für Technik und Wirtschaft Berlin
Adresse:
http://home.fhtw-berlin.de/~s0146426/Ueberblick%20Hacktools.htm
Inhalt: Computerviren
Vandals und Trojanische Pferde
Cracking
Telefon Phreaking
Netzwerk Hacking
Kommentare: Kostenlos, alles Wichtige über Computerviren.

Dipl.-Inform.Hans-Dieter Weckmann
Adresse:
http://www.uni-duisburg.de/HRZ/HRZ-Personal/weckmann/Bugs/sld001.htm
Inhalt: Computerviren
Kommentare: Kostenlos, eine interessante Einführung in das Problem „Computerviren".

Freie Universität Berlin: Arbeitsschutz- und Umweltschutzinfos
FB Chemie - Institut für Organische Chemie, Dr. Lehmann
Adresse: http://userpage.chemie.fu-berlin.de/~tlehmann/sicindex.html
Inhalt: Gefahrstoffe: Betriebsanweisungen
Laborpraxis
Kataster / Chemikalienbörse

Entsorgung von Chemikalien
Sicherheitsdaten
Gefahrstoffrecht
Unfälle, Erste Hilfe
Lernhilfen zur Arbeitssicherheit
Sonstiges:
Textfloskeln für Begehungsberichte
Aktuelle Referate, Berichte
Andere WWW-Anbieter

Anmerkungen: Kostenfrei, sehr umfangreich

Technische Universität Berlin(TUB): Sicherheitstechnische Dienste und Umweltschutz

Adresse: http://www.zrz.tu-berlin.de/~sdu/home.html

Inhalt: Arbeitsschutz
- Büroarbeitsplatze
- Gefahrstoffe
- Labore und Werkstätten
- Persönliche Schutzausrüstung
- Laser

Umweltschutz
- Grundwasserschutz (VAwS)
- Chemikalienverzeichnis
- Loseblattsammlung Umweltschutz
- Abfall
- Sonderabfall-Sammelstellenliste
- Sonderabfall-Entsorgungsauftrags-Formular
- Stromsparen

Strahlenschutz
- Strahlenschutzanweisung der TU Berlin

Brandschutz
- Brandschutzordnung der TU Berlin

Anmerkungen: Zu allen Bereichen werden die gesetzlichen Grundlagen als Links zu Umwelt-Online angeboten. Kostenfrei sind die Berlin eigenen Regelungen/Kommentare und praktischen Tipps, die teilweise im PDF-Format (Acrobat-Reader erforderlich) angeboten werden.

Universität Erlangen: Referat Umwelttechnik Sicherheitswesen

Adresse: http://www.uni-erlangen.de/docs/FAU/zuv/ref_V_5/

Schwerpunkte: Sondermüllentsorgung
Chemikalienbörse
Katastrophenschutz

Anmerkungen: Kostenfrei, besteht großteils aus Links zu anderen Quellen.

Universität Hamburg: Referat Arbeitssicherheit und Umweltschutz

Adresse: http://www.rrz.uni-hamburg.de/ar-um/

Schwerpunkte: Handbuch für Arbeitssicherheit und Umweltschutz
Betriebsanweisungen
Brandschutzordnung (im pdf-Format)

Anmerkungen: Kostenfrei, vieles (mittlerweile) nur zugänglich für Angehörige der Universität Hamburg.

Bergische Gesamthochschule Wuppertal – Fachbereich Sicherheitstechnik

Adresse: http://www.uni-wuppertal.de/FB14/welcome.html

Fachgebiete: Angewandte Verkehrssicherheitstechnik
Arbeitsphysiologie, Arbeitsmedizin und Infektionsschutz
Arbeitssicherheit und Ergonomie
Brand- und Explosionsschutz
Entwicklungs- und Konstruktionstechnik
Gefährliche Stoffe, chemische Prozesse und Konsequenzanalyse
Methoden der Sicherheitstechnik und Unfallforschung (k.S.)
Persönliche Schutzausrüstung
Produktsicherheit und Qualitätswesen
Sicherheitstechnik/Arbeitssicherheit
Sicherheitstechnik/Materialkunde
Sicherheitstechnik/Umweltschutz
Sicherheitstechnische Bauelemente
Sicherheitstechni. Messwesen und technische Diagnostik (k.S.)
Sicherheitstechnische Regelungs- und Messtechnik
Sicherheitstheorie und Verkehrstechnik
Systematische Sicherheitswissenschaft
Verkehrssicherheitstechnik

Anmerkungen: k.S.= keine eigenen Seiten vorhanden. Kostenfrei.

Bayerische Julius-Maximilians-Universität Würzburg

Adresse:	http://www.zv.uni-wuerzburg.de/datenschutz/ http://www.uni-wuerzburg.de/zv/abt7/
Inhalt:	Datenschutz Abfallentsorgung Gefahrstoffe Strahlenschutz Umweltschutz Arbeitsschutz Unfallverhütung Biologische Sicherheit Gentechnik Tierschutz
Bemerkungen:	Kostenlos. Dort oder von dort aus findet man alles zum Datenschutz. Betriebsanweisungen sind einsehbar (noch!) Viele nützliche Links.

Universität Mainz: Dienststelle Umwelt- und Arbeitsschutz

Adresse: http://www.verwaltung.uni-mainz.de/kanzler/dua/index.html

Schwerpunkt:	Gefahrstoffe	Laborgeräte Werkstätten Betriebsanweisungen Richtlinien Sicherheitsdatenblätter Gefährdungsbeurteilungsbogen
Anmerkungen:	Kostenlos. Viele interessante Dinge (z.B. Betriebsanweisungen) sind mittlerweile nur noch hochschulintern einsehbar. Sicherheitsdatenblätter als Link zu Merck. Merkblätter sind weiterhin einsehbar.	

Deutsches Krebsforschungszentrum Heidelberg

Stabsstelle Sicherheit / Abt. S0400

Adresse:	http://www.dkfz-heidelberg.de/abt2114/sichheit.htm
Schwerpunkt:	Sicherheitslexikon Verschiedene Vorschriften Links
Anmerkungen:	Kostenlos. Im Verhältnis zu anderen wenig Links aber alle wichtig!

Öffentliche Stellen

Bundesministerium für Arbeit und Sozialordnung

Adresse: http://www.bma.bund.de/

Schwerpunkte: Arbeitsrecht
Arbeitsschutz / Unfallverhütung

Anmerkungen: Kostenlos. Gesetze und Verordnungen zu Arbeitsrecht und Arbeitsschutz können im Volltext eingesehen werden.

Deutsches Informationsnetzwerk Sicherheit und Gesundheitsschutz am Arbeitsplatz

Adresse: http://de.osha.eu.int/legislation/index.stm

Schwerpunkte: Arbeitsschutz
Unfallverhütungsvorschriften (UVV)

Anmerkungen: Kostenlos. Gesetze und Verordnungen zu Arbeitsschutz und Gefahrstoffen können im Volltext eingesehen werden. Die UVVen können nicht eingesehen werden.

Land Hessen - Gesellschaft Arbeit und Ergonomie - online e.V.

Adresse: http://www.sozialnetz-hessen.de/ergo-online/ergo_frame1.htm

Schwerpunkte: Bildschirmarbeitsplätze

Anmerkungen: Kostenlos. Eine gute Informationsquelle mit vielen Tipps und Anregungen zu Bildschirmarbeitsplätzen.

Land Nordrhein-Westfalen

Adresse: http://www.arbeitsschutz.nrw.de/

Schwerpunkte: rechtliche Grundlagen
Praxistipps zu
- Schadensfälle im Betrieb: Meldewege im Regierungsbezirk Detmold
- Arbeitsorganisation
- Arbeitszeiten modern gestalten
- Arbeitsstätten
- Flucht- und Rettungswege
- Klimaanlagen/RLT-Anlagen
- Belastungen am Arbeitsplatz
- stoffliche Belastungen
- mechanische Belastungen, Lärm, Erschütterungen

ionisierende Strahlen
Gefährdungsbeurteilung am Arbeitsplatz
Bildschirm-Fragebogen (Institut ASER, Wuppertal)

Anmerkungen: Kostenlos. Gesetzliche Grundlagen als Links. Download-Angebote:
Formulare der Bezirksregierung Düsseldorf:

- Zu Arbeitsschutz
- Zu Immissionsschutz

Klima: Klimarechner
Heben und Tragen: Heben und Tragen-Rechner

Berufsgenossenschaftliches Institut für Arbeitssicherheit (BIA)

Adresse: http://www.hvbg.de/d/bia/start.htm

Inhalt: Verzeichnis krebserzeugender, erbgutverändernder oder fortpflanzungsgefährdender Stoffe (KMR-Liste)
Die Gefahrstoffdatenbank im Gefahrstoffinformationssystem der gewerblichen Berufsgenossenschaften (**GESTIS-Stoffdatenbank**)
Sicherheits-Check für Büroarbeitsplätze als praxisnahe Hilfestellung zur Gefährdungsbeurteilung.
European Information System for Occupational Safety and Health - EISOSH: Expertensystem und Dokumentation zu Persönlichen Schutzausrüstungen, Auswahl von Gehörschützern
Die Informationsstelle für Sicherheitsdatenblätter (ISI) stellt Sicherheitsdatenblätter zu chemischen Produkten zur Verfügung.

Anmerkungen: Kostenlos. Programme zum Herunterladen.
Gefahrstoffdatenbank GESTIS online!!

BASI - Bundesarbeitsgemeinschaft für Arbeitssicherheit

Adresse: http://www.basi.de/

Schwerpunkt: interessante und wichtige Links

Anmerkungen: Kostenlos

Hauptverband der gewerblichen Berufsgenossenschaften

Adresse: http://www.hvbg.de/

Schwerpunkt: aktuelle Informationen
Links

Anmerkungen: Kostenlos

HIS-Hochschul Informations System: Umweltschutz- Arbeitssicherheit

Adresse: http://www.his.de/doku/abereich/umwelt/infoseite/ind.htm

Inhalt: aktuelle Informationen
Links

Anmerkungen: Kostenlos, wohl die umfangreichste Linksammlung

Private Verbände

VDI Verein Deutscher Ingenieure

Adresse: http://www.vdi.de/

Schwerpunkte: Aktuelle Informationen
Links zu anderen Institutionen

Anmerkungen: Kostenlos

VDSI Verband Deutscher Sicherheitsingenieure e.V.

Adresse: http://www.vdsi.de/index.html

Schwerpunkte: Aktuelle Informationen
Links zu anderen Institutionen

Anmerkungen: Kostenlos

VDRI Verband Deutscher Revisionsingenieure e.V.

Adresse: http://www.vdri.de/

Schwerpunkte: Aktuelle Informationen
Links zu anderen Institutionen

Anmerkungen: Kostenlos

<u>*Deutscher Gewerkschaftsbund (DGB)*</u>

Adresse: http://www.dgb.de/

Inhalt: Links (insbesondere zu den Einzelgewerkschaften)
Aktuelle Informationen

Anmerkungen: Kostenlos, mit Stichwortsuche

<u>*IG-Metall Bildungsstätte Lohr*</u>

Adresse: http://www2.igmetall.de/netzwerke/lohr/3/1/index.html

Inhalt: Aktuelle Urteile zu Bildschirmarbeitsplätzen/SAP
BetrVG
BDSG
BV-Struktur
Arbeitsschutzgesetz
Bildschirmverordnung
SAP-Anwendung

Anmerkungen: Kostenlos, teilweise mit Links zu anderen Seiten.

Firmen

<u>*Leuwico GmbH*</u> <u>*Wiesenfeld/Coburg*</u>

Adresse: http://www.leuwico.de/web_d/Ergonomie/ER_EF_00.htm

Inhalt: Ergonomie am Bildschirmarbeitsplatz
Bildschirmarbeitsplätze
Planungsservice

Anmerkungen: Kostenlos, eine informative und humorvolle Einführung zur Bildschirmergonomie. Kontaktaufnahme über das Internet möglich.

<u>*Jedermann-Verlag Dr. Otto Pfeffer OHG*</u>

Adresse: http://www.jedermann.de/wuw.html

Inhalt: Kompendium Arbeitsschutz
CD-ROMs mit Regelwerken und Hilfsprogrammen
Sicheres Arbeiten im Labor
BETRAN – Betriebsanweisungen erstellen
Symbolbibliothek

Foliensätze auf CD – Lehrmaterial für Unterweisungen

Anmerkungen: Kostenfreie Überblicksinformation, neueste Nachrichten aus diesem Themenbereich, Bestellung über Internet möglich.

BC GmbH Verlags-, Medien-, Forschungs- und Beratungsgesellschaft Wiesbaden

Adresse: http://www.bc-verlag.de/uvv.htm

Schwerpunkt: Arbeitsschutzrecht – UVVen

Bemerkungen: Kostenlos. **Die UVVen können eingesehen werden**!!

WEKA Fachverlag, Augsburg

Adresse: http://www.ftf.weka.de/

Inhalt:	Arbeitsschutz	Rechtsgrundlagen EDV-Unterstützung Ergonomie (Büro, Maschinen, Anlagen) Gefahrstoffe
	Umweltschutz	Rechtsgrundlagen Abfall Gefahrguttransport Gewässerschutz Tipps zur Störfallverordnung

Anmerkungen: Kostenfreie Überblicksinformation, neueste Nachrichten aus diesem Themenbereich, Probesoftware kann runtergeladen werden. Bestellung über Internet möglich.

Rollo-Huber Sonnenschutz Ulm

Adresse: http://www.rollo-huber.de/index.html

Inhalt: Sonnenblenden

Anmerkungen: Kostenlose Infos zu Blendschutz an Computerarbeitsplätzen.

DIN- Deutsches Institut für Normung e.V. – Beuth Verlag Berlin

Adresse: http://www.beuth.de/

Inhalt:	Datenbanken	PERINORM DIN-Katalog DIN-TERM
	Normensammlungen	DIN-Individuell DIN-Fachgebiete

DIN-Gruppen
Technisches Recht
VDI-Richtlinien
DIN EN IS0 9000 ff.
Maschinensicherheit
VDE-Vorschriftenwerk

Beuth-Kommentare
Loseblattausgaben

Anmerkungen: Kostenlose Produktübersicht. Hier findet man eine komplette Übersicht über alle Normen, Bestellung über Internet möglich.

G.U.B. Gesellschaft für Unternehmensberatung mbH

Adresse: http://wauplus.ckc.de/

Schwerpunkt: Softwarepaket WAU-Plus
Abfallmanagement
Betrieblicher Arbeitsschutz
Gefahrstoffmanagement
Gefahrgutmanagement
Betriebl. Unfallbearbeitung
Anlagenkataster nach VAwS

Anmerkungen: Kostenlos, sehr gutes Informationsmaterial zum Programm WAU-Plus

Kroschke sign-international GmbH, Braunschweig

Adresse: http://www.kroschke.com/frameset.html

Inhalte: Schutzkleidung,
Schutzvorrichtungen,
Schilder

Anmerkungen: Kostenlos, ein recht großes Angebot im Bereich Arbeits- und Umweltschutz. Bestellungen über Internet möglich, Privatpersonen können nicht bestellen.

Umwelt-Online

Adresse:	http://www.umwelt-online.de/homepage.htm?
Inhalte:	Anbieter-Datenbank mit über 2000 Anbietern Regelwerk zum Arbeits- , Umweltschutz, Gefahrguttransport- und Technikrecht
Anmerkungen:	Teilweise kostenlos (Recherche in Anbieterdatenbank), teilweise wird Benutzernummer und Paßwort verlangt (Regelwerk).

DRÄGER - Sicherheitstechnik, Lübeck

Adresse:	http://www.draeger.com/german/st/index.htm
Inhalte:	Analytik Atem- Alkoholmeßtechnik Atem- und Körperschutz Gasmeß- und Gaswarntechnik Tauchen Feuerwehr Wohnraummessung Gefahrstoffdatenbank Drägerheft
Anmerkungen:	Kostenlos, sehr gutes Informationsmaterial zur Produktpalette. Das Drägerheft enthält aktuelle Nachrichten zu Gefahrstoffen, Messtechnik und Arbeitsschutz allgemein. Bestellung über Internet möglich.

Carl Heymanns Verlag, Köln

Adresse:	http://www.heymanns.com/
Schwerpunkt:	Unfallverhütungsvorschriften Technische Regelwerke
Anmerkungen:	Kostenlos, Bestellung über Internet möglich.

Universum Verlagsanstalt

Adresse:

http://www.universum.de/univ/arbeit_gesundheit/index_ag_main.html

Schwerpunkt:	Arbeitsschutzzeitschriften Sicherheitskalender
Anmerkungen:	Kostenlos, Bestellungen über Internet möglich.

Merck KGaA, Darmstadt

Adresse:	http://www.merck.de/german/services/ http://chemdat.merck.de/	
Inhalte:	Analytische Reagenzien	Säuren z.A. Ätzalkalien und Laugen Anorganische Salze
	Chromatographie Umweltanalytik Mikrobiologie Chemikaliendatenbank mit Sicherheitsdatenblätter:	
	- ChemDAT online:	Product information Safety Data Sheets Technical Data Sheets
Anmerkungen:	Kostenlos, sehr gutes Informationsmaterial zur Produktpalette. Bestellung über Internet möglich. Humorvolle, ausführliche Informationen zu Säuren, Ätzalkalien und Laugen. **Chemikaliendatenbank (ChemDat) ist einsehbar**! (auf Englisch) Die Sicherheitsdatenblätter (Safety Data Sheets) werden viersprachig (Deutsch, Englisch, Französisch, Spanisch) als Pdf-File (Acrobat-Reader notwendig) angeboten.	

Anhang 3-1

Verordnung über Sicherheit und Gesundheitsschutz bei der Arbeit an Bildschirmgeräten

(Bildschirmarbeitsverordnung - BildscharbV)

§ 1

Anwendungsbereich

(1) Diese Verordnung gilt für die Arbeit an Bildschirmgeräten.

(2) Diese Verordnung gilt nicht für die Arbeit an

1. Bedienerplätzen von Maschinen oder an Fahrerplätzen von Fahrzeugen mit Bildschirmgeräten,
2. Bildschirmgeräten an Bord von Verkehrsmitteln,
3. Datenverarbeitungsanlagen, die hauptsächlich zur Benutzung durch die Öffentlichkeit bestimmt sind,
4. Bildschirmgeräten für den ortsveränderlichen Gebrauch, sofern sie nicht regelmäßig an einem Arbeitsplatz eingesetzt werden,
5. Rechenmaschinen, Registrierkassen oder anderen Arbeitsmitteln mit einer kleinen Daten- oder Messwertanzeigevorrichtung, die zur unmittelbaren Benutzung des Arbeitsmittels erforderlich ist, sowie
6. Schreibmaschinen klassischer Bauart mit einem Display.

(3) Die Verordnung gilt nicht in Betrieben, die dem Bundesberggesetz unterliegen.

(4) Das Bundeskanzleramt, das Bundesministerium des Innern, das Bundesministerium für Verkehr, das Bundesministerium der Verteidigung oder das Bundesministerium der Finanzen können, soweit sie hierfür jeweils zuständig sind, im Einvernehmen mit dem Bundesministerium für Arbeit und Sozialordnung und, soweit nicht das Bundesministerium des Innern selbst zuständig ist, im Einvernehmen mit dem Bundesministerium des Innern bestimmen, dass für bestimmte Tätigkeiten im öffentlichen Dienst des Bundes, insbesondere bei der Bundeswehr, der Polizei, den Zivil- und

Katastrophenschutzdiensten, dem Zoll oder den Nachrichtendiensten, Vorschriften dieser Verordnung ganz oder zum Teil nicht anzuwenden sind, soweit öffentliche Belange dies zwingend erfordern, insbesondere zur Aufrechterhaltung oder Wiederherstellung der öffentlichen Sicherheit. In diesem Fall ist gleichzeitig festzulegen, wie die Sicherheit und der Gesundheitsschutz der Beschäftigten nach dieser Verordnung auf andere Weise gewährleistet werden.

§ 2

Begriffsbestimmungen

(1) Bildschirmgerät im Sinne dieser Verordnung ist ein Bildschirm zur Darstellung alpha-numerischer Zeichen oder zur Grafikdarstellung, ungeachtet des Darstellungsverfahrens.

(2) Bildschirmarbeitsplatz im Sinne dieser Verordnung ist ein Arbeitsplatz mit einem Bildschirmgerät, der ausgestattet sein kann mit

1. Einrichtungen zur Erfassung von Daten,
2. Software, die den Beschäftigten bei der Ausführung ihrer Arbeitsaufgaben zur Verfügung steht,
3. Zusatzgeräten und Elementen, die zum Betreiben oder Benutzen des Bildschirmgeräts gehören, oder
4. sonstigen Arbeitsmitteln,

sowie die unmittelbare Arbeitsumgebung.

(3) Beschäftigte im Sinne dieser Verordnung sind Beschäftigte, die gewöhnlich bei einem nicht unwesentlichen Teil ihrer normalen Arbeit ein Bildschirmgerät benutzen.

§ 3

Beurteilung der Arbeitsbedingungen
Bei der Beurteilung der Arbeitsbedingungen nach § 5 des Arbeitsschutzgesetzes hat der Arbeitgeber bei Bildschirmarbeitsplätzen die Sicherheits- und Gesundheitsbedingungen insbesondere hinsichtlich einer möglichen Gefährdung des Sehvermögens sowie körperlicher Probleme und psychischer Belastungen zu ermitteln und zu beurteilen.

§ 4

Anforderungen an die Gestaltung

(1) Der Arbeitgeber hat geeignete Maßnahmen zu treffen, damit die Bildschirmarbeitsplätze den Anforderungen des Anhangs und sonstiger Rechtsvorschriften entsprechen.

(2) Bei Bildschirmarbeitsplätzen, die bis zum 20. Dezember 1996 in Betrieb sind, hat der Arbeitgeber die geeigneten Maßnahmen nach Absatz 1 dann zu treffen,

1. wenn diese Arbeitsplätze wesentlich geändert werden oder
2. wenn die Beurteilung der Arbeitsbedingungen nach § 3 ergibt, dass durch die Arbeit an diesen Arbeitsplätzen Leben oder Gesundheit der Beschäftigten gefährdet ist,

spätestens jedoch bis zum 31. Dezember 1999.

(3) Von den Anforderungen des Anhangs darf abgewichen werden, wenn

1. die spezifischen Erfordernisse des Bildschirmarbeitsplatzes oder Merkmale der Tätigkeit diesen Anforderungen entgegenstehen oder
2. der Bildschirmarbeitsplatz entsprechend den jeweiligen Fähigkeiten der daran tätigen Behinderten unter Berücksichtigung von Art und Schwere der Behinderung gestaltet wird, und dabei Sicherheit und Gesundheitsschutz auf andere Weise gewährleistet sind.

§ 5

Täglicher Arbeitsablauf
Der Arbeitgeber hat die Tätigkeit der Beschäftigten so zu organisieren, dass die tägliche Arbeit an Bildschirmgeräten regelmäßig durch andere Tätigkeiten oder durch Pausen unterbrochen wird, die jeweils die Belastung durch die Arbeit am Bildschirmgerät verringern.

§ 6

Untersuchung der Augen und des Sehvermögens

(1) Der Arbeitgeber hat den Beschäftigten vor Aufnahme ihrer Tätigkeit an Bildschirmgeräten, anschließend in regelmäßigen Zeitabständen sowie bei Auftreten von Sehbeschwerden, die auf die Arbeit am Bildschirmgerät zurückgeführt werden können, eine angemessene Untersuchung der Augen und des Sehvermögens durch eine fachkundige Person anzubieten. Erweist sich auf Grund der Ergebnisse einer Untersuchung nach Satz 1 eine augenärztliche Untersuchung als erforderlich, ist diese zu ermöglichen.

(2) Den Beschäftigten sind im erforderlichen Umfang spezielle Sehhilfen für ihre Arbeit an Bildschirmgeräten zur Verfügung zu stellen, wenn die Ergebnisse einer Untersuchung nach Absatz 1 ergeben, dass spezielle Sehhilfen notwendig und normale Sehhilfen nicht geeignet sind.

§ 7

Ordnungswidrigkeiten
Ordnungswidrig im Sinne des § 25 Abs. 1 Nr. 1 des Arbeitsschutzgesetzes handelt, wer vorsätzlich oder fahrlässig entgegen § 6 Abs. 1 Satz 1 die dort bezeichneten Untersuchungen nicht oder nicht rechtzeitig anbietet.

Anhang

über an Bildschirmarbeitsplätze zu stellende Anforderungen

Bildschirmgerät und Tastatur

1. Die auf dem Bildschirm dargestellten Zeichen müssen scharf, deutlich und ausreichend groß sein sowie einen angemessenen Zeichen- und Zeilenabstand haben.
2. Das auf dem Bildschirm dargestellte Bild muss stabil und frei von Flimmern sein; es darf keine Verzerrungen aufweisen.
3. Die Helligkeit der Bildschirmanzeige und der Kontrast zwischen Zeichen und Zeichenuntergrund auf dem Bildschirm müssen einfach einstellbar sein und den Verhältnissen der Arbeitsumgebung angepasst werden können.
4. Der Bildschirm muss frei von störenden Reflexionen und Blendungen sein.

5. Das Bildschirmgerät muss frei und leicht drehbar und neigbar sein.
6. Die Tastatur muss vom Bildschirmgerät getrennt und neigbar sein, damit die Benutzer eine ergonomisch günstige Arbeitshaltung einnehmen können.
7. Die Tastatur und die sonstigen Eingabemittel müssen auf der Arbeitsfläche variabel angeordnet werden können. Die Arbeitsfläche vor der Tastatur muss ein Auflegen der Hände ermöglichen.
8. Die Tastatur muss eine reflexionsarme Oberfläche haben.
9. Form und Anschlag der Tasten müssen eine ergonomische Bedienung der Tastatur ermöglichen. Die Beschriftung der Tasten muss sich vom Untergrund deutlich abheben und bei normaler Arbeitshaltung lesbar sein.

Sonstige Arbeitsmittel

1. Der Arbeitstisch bzw. die Arbeitsfläche muss eine ausreichend große und reflexionsarme Oberfläche besitzen und eine flexible Anordnung des Bildschirmgeräts, der Tastatur, des Schriftguts und der sonstigen Arbeitsmittel ermöglichen. Ausreichender Raum für eine ergonomisch günstige Arbeitshaltung muss vorhanden sein. Ein separater Ständer für das Bildschirmgerät kann verwendet werden.
   Der Arbeitsstuhl muss ergonomisch gestaltet und standsicher sein.
2. Der Vorlagenhalter muss stabil und verstellbar sein sowie so angeordnet werden können, dass unbequeme Kopf- und Augenbewegungen soweit wie möglich eingeschränkt werden.
3. Eine Fußstütze ist auf Wunsch zur Verfügung zu stellen, wenn eine ergonomisch günstige Arbeitshaltung ohne Fußstütze nicht erreicht werden kann.

Arbeitsumgebung

1. Am Bildschirmarbeitsplatz muss ausreichender Raum für wechselnde Arbeitshaltungen und -bewegungen vorhanden sein.
2. Die Beleuchtung muss der Art der Sehaufgabe entsprechen und an das Sehvermögen der Benutzer angepasst sein; dabei ist ein angemessener Kontrast zwischen Bildschirm und Arbeitsumgebung zu gewährleisten. Durch die Gestaltung des Bildschirmarbeitsplatzes sowie Auslegung und Anordnung der Beleuchtung sind störende Blendwirkungen, Reflexionen oder Spiegelungen auf dem Bildschirm und den sonstigen Arbeitsmitteln zu vermeiden.
3. Bildschirmarbeitsplätze sind so einzurichten, dass leuchtende oder beleuchtete Flächen keine Blendung verursachen und Reflexionen auf dem Bildschirm soweit wie möglich vermieden werden. Die Fenster müssen mit einer geeigneten verstellbaren Lichtschutzvorrichtung ausgestattet

sein, durch die sich die Stärke des Tageslichteinfalls auf den Bildschirmarbeitsplatz vermindern lässt.

4. Bei der Gestaltung des Bildschirmarbeitsplatzes ist dem Lärm, der durch die zum Bildschirmarbeitsplatz gehörenden Arbeitsmittel verursacht wird, Rechnung zu tragen, insbesondere um eine Beeinträchtigung der Konzentration und der Sprachverständlichkeit zu vermeiden.
5. Die Arbeitsmittel dürfen nicht zu einer erhöhten Wärmebelastung am Bildschirmarbeitsplatz führen, die unzuträglich ist. Es ist für eine ausreichende Luftfeuchtigkeit zu sorgen.
6. Die Strahlung muss - mit Ausnahme des sichtbaren Teils des elektromagnetischen Spektrums - so niedrig gehalten werden, dass sie für Sicherheit und Gesundheit der Benutzer des Bildschirmgerätes unerheblich ist.

Zusammenwirken Mensch - Arbeitsmittel

1. Die Grundsätze der Ergonomie sind insbesondere auf die Verarbeitung von Informationen durch den Menschen anzuwenden.
2. Bei Entwicklung, Auswahl, Erwerb und Änderung von Software sowie bei der Gestaltung der Tätigkeit an Bildschirmgeräten hat der Arbeitgeber den folgenden Grundsätzen insbesondere im Hinblick auf die Benutzerfreundlichkeit Rechnung zu tragen:
   - 2.1. Die Software muss an die auszuführende Aufgabe angepaßt sein.
   - 2.2. Die Systeme müssen den Benutzern Angaben über die jeweiligen Dialogabläufe unmittelbar oder auf Verlangen machen.
   - 2.3. Die Systeme müssen den Benutzern die Beeinflussung der jeweiligen Dialogabläufe ermöglichen sowie eventuelle Fehler bei der Handhabung beschreiben und deren Beseitigung mit begrenztem Arbeitsaufwand erlauben.
   - 2.4. Die Software muss entsprechend den Kenntnissen und Erfahrungen der Benutzer im Hinblick auf die auszuführende Aufgabe angepaßt werden können.

Ohne Wissen der Benutzer darf keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden.

Anhang 3-2

Zum Geltungsbereich der Bildschirmarbeitsverordnung

Generell:

- Gültig für alle Arbeitsplätze mit Bildschirmgerät.
- Gültig für alle Beschäftigte, für deren Arbeit das Bildschirmgerät nicht unwesentlich ist.
- Gültig für alle Betriebe in Produktion und Dienstleistung, außer für Bergbaubetriebe.
- Nicht gültig für:
    - Maschinenbedienplätze
    - Geräte in Verkehrsmitteln
    - Geräte für die Öffentlichkeit.
    - Kassen mit kleiner Datenanzeige
    - Display-Schreibmaschinen
    - Videoüberwachung.
- Für ortsveränderliche Bildschirmgeräte, die nicht regelmäßig am Arbeitsplatz benutzt werden gilt sie ebenfalls nicht.

Was ist ein Bildschirmarbeitsplatz im Sinne der Bildschirmverordnung?

- Ein Bildschirmarbeitsplatz ist ein Arbeitsplatz mit Bildschirmgerät, Software und Zubehör sowie die unmittelbare Arbeitsumgebung. Für ihn gelten die Anforderungen an die Gestaltung aus der BildschArbV, insbesondere des Anhangs.

Beispiele sind:

- Texterfassung mit Hilfe von EDV
- Sachbearbeitung mit Computerhilfe
- regelmäßig genutzte (Computer-)Arbeitsplätze von Außendienstmitarbeitern im Betrieb
- Leitstände
- Computerkassen
- Laufbildbearbeitung

Nicht alle Arbeitsplätze, die mit Computer und/oder Bildschirm ausgestattet sind und nicht alle Beschäftigte, die mit EDV arbeiten, fallen unter die Bestimmungen der Bildschirmarbeitsverordnung. Wenn keine Gesundheitsgefahren für die Beschäftigten zu erwarten sind, muss der Arbeitsplatz nicht die Anforderungen der Verordnung erfüllen. Es gelten weiterhin noch folgende Ausnahmen:

- Bedienerplätze von Maschinen (Steuereinrichtungen)

- Bedienerplätze in Fahrzeugen und anderen Verkehrsmitteln
- Bildschirmgeräte für die Öffentlichkeit
- ortsveränderliche Bildschirme die nicht regelmäßig am Arbeitsplatz eingesetzt werden, wie Laptops, Notebooks
- Rechenmaschinen, Registrierkassen
- Messwertanzeigen, die nur zur unmittelbaren Benutzung des Arbeitsmittels erforderlich sind
- Bildschirme zur Videoüberwachung
- wenn es sich um eine spezielle Tätigkeit oder Behindertenarbeitsplätze handelt und der Gesundheitsschutz anders gesichert wird

Die Anforderungen der Bildschirmarbeits-Verordnung gelten für alle Beschäftigten, die gewöhnlich bei einem nicht unwesentlichen Teil ihrer normalen Arbeit ein Bildschirmgerät benutzen.

Die beschriebenen Ausnahmen sind eine Auslegung des Gesetzestextes, aber nicht im Gesetz selbst bestimmt:

- Beschäftigte die täglich weniger als 5 -25 % ihrer normalen Arbeitszeit ein Bildschirmgerät benutzen.
- Beschäftigte für deren Tätigkeit das Bildschirmgerät nicht zwingend ist, die dafür keine besonderen Kenntnisse benötigen, denen dabei auch keine Aufmerksamkeit abverlangt wird oder die nie ununterbrochen mindestens eine Stunde täglich am Bildschirm arbeiten.

Auslegung des Gesetzestextes nach HBV

Die HBV geht davon aus, dass „Bildschirme, die direkt an einer Maschine oder einem Arbeitsmittel allein zu deren Benutzung angebracht sind, nicht unter die Verordnung fallen, dagegen aber Bildschirme zur Steuerung oder Überwachung von verfahrenstechnischen Anlagen.“/HBV/

Nach HBV ist der Gesetzestext zur Definition von Beschäftigen im Sinne der Bildschirmarbeitsverordnung nicht eindeutig. Der Satz: "Gewöhnlich bei einem nicht unwesentlich Teil der normalen Arbeit", erfordert eine Interpretation. Die HBV greift hierzu auf parallele Regelungen im nationalen Recht zurück. „Im Wahlrecht sind Parteien nicht unwesentlich, wenn sie 5% der Stimmen haben;

im Aktienrecht sind Aktionäre nicht unwesentlich, die wenigstens 10% der Stimmen haben; im GmbH-Recht gibt es Grenzen von 10% - 25%. Gehen wir davon aus, dass irgendwo zwischen 5% bis 25% der Arbeitszeit auch die Grenze zu „unwesentlich“ anzusetzen ist, dann sind das bei einem 8-Stunden-Arbeitstag 1 bis 2 Stunden.“/HBV/

Die HBV zitiert den Entwurf der Unfallverhütungsvorschrift VGB 104 „Arbeit an Bildschirmgeräten“ der Berufsgenossenschaften. Hier wird darauf verwiesen, dass drei von vier der im folgenden aufgeführten Kriterien erfüllt sein müssen, um von Beschäftigten im Sinne der Verordnung sprechen zu können:

„Definition von Beschäftigten im Sinne der BildschArbV nach Berufsgenossenschaft:
- Zur Durchführung der Arbeit wird ein Bildschirmgerät zwingend benötigt.
- Besonderer Kenntnisse und Fähigkeiten zur Bildschirmarbeit sind notwendig.
- Der Bildschirm wird mehrmals arbeitstäglich in ununterbrochenen Zeitabschnitten von mindestens einer Stunde benutzt.
- Die Arbeit verlangt hohe Aufmerksamkeit und Konzentration, weil Fehler zu wesentlichen Konsequenzen führen können.

Eine weitere Veröffentlichung der Verwaltungs-Berufsgenossenschaft verweist darauf, dass es Arbeiten sind, die ohne Bildschirmunterstützung nicht zu erledigen sind. (G37 - Berufsgenossenschaftlicher Grundsatz für arbeitsmedizinische Vorsorgeuntersuchungen SP 5.3 1997) “/HBV/

Die HBV gibt in ihrer Interpretation der Verordnung folgende wichtige Ausnahmen an:

spezielle Tätigkeitsmerkmale
Ausnahmen sind möglich, wenn spezielle Merkmale einer Tätigkeit den Mindestanforderungen an die Gestaltung der Arbeitsplätze entgegen stehen. Der Gesundheitsschutz muss dann auf andere Weise gewährleistet werden. Die HBV erwähnt als Beispiel den Kundenservicebereich, „weil hier Steharbeitsplätze mit geringer Tischtiefe eingesetzt werden und normale Bürostühle nicht verwendbar sind.“/HBV/ Es wird empfohlen in solchen Fällen Gesundheitsgefährdungen durch andauerndes Stehen zu vermeiden, indem eine Stehhilfe oder ein entsprechend hoher Stuhl mit Fußstütze zur Verfügung gestellt wird.

Behinderten-Arbeitsplätze
Abhängig von der Art der Körperbehinderung sind für Behinderte entsprechend angepasste Sonderkonstruktionen von Tisch, Stuhl oder Bildschirmgeräten notwendig. Es muss geprüft werden, wie in solchen Fällen

ein ausreichender Gesundheitsschutz an diesen speziellen Behindertenarbeitsplätzen gewährleistet werden kann.

Notebook
Notebooks sind ortsveränderliche Computer. Diese werden immer häufiger eingesetzt. Werden Notebooks regelmäßig an einem festen Arbeitsplatz verwendet, gelten hier ebenso die Anforderungen der Verordnung. Die Notebooks müssen dann also über eine sogenannte Docking-Station (Anschlussmöglichkeit für ein Notebook) an einen getrennten Bildschirm und eine getrennte Tastatur angeschlossen sein.
Gewöhnlich werden Notebooks im Außendienst, z.B. regelmäßig beim Kunden, im Hotelzimmer oder zu Hause benutzt. Ein ausreichender Gesundheitsschutz welcher den Bestimmungen zur Ausnahmeregelung entspricht, muss beispielsweise mit organisatorischen Maßnahmen gesichert werden.

`Betriebliche´ Ausnahmen
Betriebe und Verwaltungen, die dem Bundesberggesetz unterliegen als auch für Tätigkeiten des öffentlichen Dienstes bei Bundeswehr, Polizei, Zivil- und Katastrophenschutz, Zoll und Nachrichtendiensten gilt eine Ausnahmeregelung dann, wenn zwingende öffentliche Belange dies erfordern. Sicherheit und Gesundheitsschutz am Arbeitsplatz muss dann auf andere Weise gewährleistet werden.

Die HBV empfiehlt noch:
„In einer Vereinbarung mit dem Betriebs- oder Personalrat sollte festgelegt werden, für welche Arbeitsplätze und für wen Gestaltungsanforderungen, Augenvorsorge oder Recht auf Bildschirmbrille gelten.“/HBV/

Anhang 3-3

Zu Pausen bei der Bildschirmarbeit

Zusammengefasst:

- Regelmäßige Pausen gehören zur Arbeit am Bildschirm.
- Dadurch sollen die Belastungen durch die Bildschirmarbeit verringert werden.
- Pausen erhöhen die Leistungsfähigkeit, d.h. sie "lohnen" sich.
- Wichtig: Mehrere kurze Pausen sind sinnvoller als wenige lange.

Gesetzliche Regelung:
Bildschirmarbeitsverordnung
Der Arbeitgeber muss die Tätigkeit so organisieren, dass die tägliche Arbeit an Geräten mit Bildschirmen regelmäßig entweder durch andere Tätigkeiten oder durch Pausen unterbrochen wird. Damit soll erreicht werden, dass die Belastungen durch Bildschirmarbeit verringert werden.
Die Unterbrechung der Arbeit durch andere Tätigkeiten hat Vorrang vor Pausenregelungen, Mischarbeit soll bevorzugt werden. Das Bundesarbeitsministerium empfiehlt, dass der Prozentsatz der Tätigkeiten ohne Bildschirmarbeit unter 50 Prozent liegen soll.
Die Bildschirmarbeitsverordnung meint sogenannte Kurzpausen, also bezahlte Arbeitsunterbrechungen. Die im Arbeitszeitrecht geforderten Ruhepausen werden von der Verordnung nicht berührt.

Warum Pausen?
Leistungsfähigkeit und Ermüdung
Die Leistungskurve bewegt sich nach unten wenn man intensiv und konzentriert über längere Zeit arbeiten muss, wie es üblicherweise bei Bildschirmarbeit notwendig ist. Solche Arbeit macht müde und erholungsbedürftig. Die Konzentration nimmt nach einiger Zeit deutlich ab und damit nimmt die Fehlerhäufigkeit zu. Die Ermüdung zeigt sich in körperlichen Symptomen wie flacher werdende Atmung und beschleunigter Puls.

Argumente für die Einführung von Kurzpausen:

- „Pausen beseitigen Erschöpfungssymptome, die durch die Arbeit verursacht wurden.
- Sie sorgen dafür, dass keine Ermüdung entsteht.
- Sie sind keine unproduktiven Arbeitsunterbrechungen, sondern sichern und steigern die Leistungsfähigkeit.
- Sie tragen dazu bei, dass sich die Augen von den Strapazen der Bildschirmarbeit erholen.“/HBV/

Der DGB hat Untersuchungen, welche Beeinträchtigungen nach welcher Arbeitszeit am Rechner auftreten und nach welcher (Pausen-) Zeit diese Erscheinungen wieder kuriert sind:

Anhaltspunkte zur Festlegung von Erholzeiten		
Arbeitszeit am Bildschirm	Beeinträchtigungen	Wiederherstellungs-zeiten
4 Stunden	Sehschärfeminderungen Farbsinnstörungen	15-35 Min 20 Min
3 Stunden	<u>Sehschärfeminderungen</u> <u>Farbsinnstörungen</u> <u>Physische Ermüdung</u> <u>Augenermüdung</u>	10-15 Min 15 Min 15 Min
2 Stunden	<u>Akkommodations- und Adaptionsstörungen</u> Sehschärfeminderungen Farbsinnstörungen	 15 Min 15 Min
1,5 Stunden	gesundheitliche Beeinträchtigungen werden von der Mehrheit der Betroffenen angegeben (Schweden)	
1 Stunde	Sehschärfeminderungen Farbsinnstörungen	10 Min 10 Min

Quelle: Zusammenstellung aus verschiedenen Forschungsberichten, in: DGB Bundesvorstand, Angestellte und Automation, 1984, Verfasserin: A. Köchling; unterstrichene Angaben statistisch gesichert.

Anmerkung:
Führen EDV-Abstürze zu plötzlichen Wartezeiten im Arbeitsablauf, sind das keine Pausen im Sinne der Bildschirmarbeitsverordnung. Sie sind in der Regel unerwünscht, störend, nicht vorhersehbar und planbar. Derartige Zwangspausen werden von den Beschäftigten fast immer als Belastung erlebt. Statt zur Erholung bei zu tragen, nerven und frustrieren diese nur.

Was sollte man bei der Pausengestaltung beachten?

- „Der Erholungswert mehrerer kurzer Pausen ist größer als der von wenigen langen Pausen.
- Häufigkeit und Dauer der Pausen orientieren sich am Schwierigkeitsgrad der Arbeit. Je nach Arbeitsaufgabe werden 5 bis 15 Minuten pro Stunde empfohlen.
- Der Regenerationswert von Pausen darf nicht durch andere Arbeiten vermindert werden.
- Die Beschäftigten sollen die Lage ihrer Pausen frei wählen können, denn die Leistungsfähigkeit ändert sich im Laufe eines Tages und unterliegt individuellen Schwankungen.“/HBV/

Die HBV machte sich Gedanken darüber, wie man am besten den Arbeitstag eines Beschäftigten am Bildschirm aufteilt. Sie übernehmen und empfehlen folgenden Vorschlag für eine Verteilung von Kurzpausen bei Bildschirmarbeit:

Uhrzeit	Arbeitszeit (min)	Pausenzeit (min)
07:30	160	
10:00		15
	95	
12:00		45 (incl. Mittagspause)
	95	
14:00		
		15
16:00	85	

(nach Richenhagen, Bildschirmarbeitsplätze, 1996)

Noch ein Hinweis für die Beschäftigten:

- Man soll die Kurzpause nicht zeitungslesend an seinem Bildschirmgerät verbringen. Das ist ein wenig sinnvoller Gebrauch.
- Ausgleichsübungen – dies können regelrechte Gymnastikübungen sein, aber auch schon Augenübungen helfen das Ziel:
  - Entspannung und
  - Stressbewältigung

  zu erreichen.
- Körper und Psyche verlangen eigentlich Bewegung, also weg vom Bildschirm.

Anhang 3-4

Anforderungen an die Gestaltung der Bildschirmarbeit

Zusammenfassend gesagt:

- „Der Arbeitsablauf wird durch andere Tätigkeiten oder Pausen unterbrochen.
- Die Bildschirmdarstellung ist deutlich, scharf, ausreichend groß, stabil, flimmerfrei, reflexionsfrei.
- Helligkeit und Kontrast sind an individuelle Anforderungen anpassbar.
- Die Tastatur ist frei beweglich, reflexionsarm und ergonomisch bedienbar.
- Der Arbeitstisch ist ausreichend groß und reflexionsarm, der Arbeitsstuhl standsicher und ergonomisch.
- Vorlagenhalter, Ständer für den Bildschirm und Fußstütze sind stabil und verstellbar.
- Am Arbeitsplatz ist ausreichend Raum für wechselnde Bewegungen.
- Lärm wird vermieden und gutes Klima ist vorhanden.
- Der Bildschirm ist strahlungsarm.
- Informationsdarstellung und Softwaredialoge sind ergonomisch."/HBV/

Der Anhang der Bildschirmverordnung enthält allgemein formulierte ergonomische Mindestanforderungen. In Normen, Sicherheitsregeln, technischen Regeln oder Unfallverhütungsvorschriften werden diese weiter ausgeführt. Weiterhin sind das Arbeitsschutzgesetz (ArbSchG) und die Arbeitsstättenverordnung (ArbStättV) zu beachten. Insbesondere die Unfallverhütungsvorschrift VBG 104 "Arbeit an Bildschirmgeräten" hat bei der Konkretisierung berücksichtigt zu werden. Sie gilt als gesicherte arbeitswissenschaftliche Erkenntnis.

.

Arbeitsplätze, die neu geschaffen werden, müssen den Mindestanforderungen von Anfang an entsprechen. Alle anderen Bildschirmarbeitsplätze müssen seit dem 31.12.99 den Anforderungen genügen.

Die HBV hat die gesetzlichen und sonstigen Vorschriften zusammen gestellt, die bei der Gestaltung und dem Gebrauch von Bildschirmarbeitsplätzen von Interesse sind. :

Übersicht über die gesetzlichen und sonstigen Vorschriften und das technische Regelwerk

Gestaltungsfeld	BildschArbV	Gesetze, Verordnungen, technisches Regelwerk zur konkreten Ausgestaltung
Arbeitsablauf und Pausen	§ 5; § 4 Anhang Nr. 21.1-21.4	ArbschG § 4, 5; DIN 33405, DIN EN ISO 10075, DIN EN ISO9241 Teil 2; Sicherheitsregel der VBG ZH 1/618
Bildschirmgerät	§ 4, Anhang Nr. 1-5	DIN EN ISO 9241, Teile 3,8; DIN 66234 Teil 1,2,5,6,7,9; Sicherheitsregel der VBG ZH 1/618
Tastatur	§ 4, Anhang Nr. 6-9	DIN 66234 Teil 6, DIN 2136, DIN 2137, DIN 9758 u.a.; Sicherheitsregel der VBG ZH 1/618
Arbeitstisch	§ 4, Anhang Nr. 10	DIN 4543 Teil 1, DIN 4549, DIN 4554, Sicherheitsregel der VBG ZH 1/618 und ZH 1/535
Arbeitsstuhl	§ 4, Anhang Nr. 11	DIN 4551, DIN 4550, DIN 68131, DIN 68877; Sicherheitsregel der VBG ZH 1/618 und ZH 1/535
Vorlagenhalter, Fußstütze	§ 4, Anhang Nr. 12-13	DIN 4556, DIN 66234 Teil 6; Sicherheitsregel der VBG ZH 1/618 und ZH 1/535
Raum	§ 4, Anhang Nr. 14	DIN 4543 Teil 1-2, ArbStättV §§ 10,17,23,24; ArbStättR 17/1.2; Sicherheitsregel der VBG ZH 1/618 und ZH 1/535
Beleuchtung	§ 4, Anhang Nr. 15-16	ArbStättV §§7,8; ArbstättR 7/1, 7/3; DIN 5034, DIN 5035, DIN 66234 Teil 6,7, DIN 5032, DIN 5040, Sicherheitsregel der VBG ZH 1/618 und ZH 1/535 sowie ZH 1/190
Lärm	§ 4, Anhang Nr. 17	ArbStättV § 15; DIN 4109, DIN 33410, DIN EN ISO 3741, DIN EN ISO 7779; UVV VBG 121
Klima	§ 4, Anhang Nr. 18	ArbStättV §§ 5,6,9,16; ArbStättR 5, 6/1,3; DIN 1956-2, DIN 33403; Sicherheitsregel der VBG ZH 1/618 und ZH 1/535 sowie ZH 1/190
Strahlung	§ 4, Anhang Nr. 19	Röntgenverordnung, Strahlenschutz-verordnung, Gesetz über die elektromagnetische Verträglichkeit von

		Geräten (EMVG), DIN VDE 0848, DIN VDE 0870, DIN 57848, Sicherheitsregeln der VBG ZH 1/43, MPR II
Software	§ 4, Anhang Nr. 20-22	DIN EN ISO 9241 Teil 10 ff., Sicherheitsregel der VBG ZH 1/618
Augenvorsorge-untersuchung, Sehhilfe	§ 6	ArbschG § 11, UVV VBG 100 § 2, 4-9, Berufsgenossenschaftlicher Grundsatz G37

Tabelle: Gesetzliche und andere Vorschriften/HBV/

Sehr wichtig ist, dass der Arbeitgeber verpflichtet ist die Gestaltungsanforderungen einzuhalten. Wird z.B. keine Augenvorsorgeuntersuchung angeboten, so stellt das eine Ordnungswidrigkeit dar, die mit einem Bußgeld bis zu 10.000 DM geahndet werden kann

Die HBV empfiehlt folgende Literatur, um sich mit Bildschirmarbeit und der Bildschirmverordnung vertraut zu machen:

Die neue Bildschirmarbeitsverordnung: Verordnung, Kommentar, Arbeitshilfen
Hg.: Gewerkschaft Handel, Banken und Versicherungen, Industriegewerkschaft Medien, Druck und Papier, Publizistik und Kunst sowie Deutsche Postgewerkschaft, 1997

Richenhagen/Prümper/Wagner:
Handbuch der Bildschirmarbeit Luchterhand-Verlag (2. Auflage), Neuwied, Kriftel 1998

Anhang 3-5

Ergonomieprüfliste von Rechnerarbeitsplätzen /Schue/

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsumgebung** Prüfgegenstand : **Raumklima**

Arbeitsplatz : Prüfdatum :

Vorschriften : ArbstättV § 5, Röntgenverordnung

	Ja	Nein	i.A.
1. Raumtemperatur - mindestens 20°C / maximal 23°C (in Spitzen maximal 26°C)	❑	❑	
2. Relative Luftfeuchtigkeit - im Bereich von 50% bis 65%	❑	❑	
3. Luftgeschwindigkeit - Maximalwert 0,1 bis 0,15 m/sec	❑	❑	
4. Belastungsstrahlung	❑	❑	
5. Geruchsbelästigung	❑	❑	❑

Maßnahmen :	Frist :
______________________	__________
______________________	__________
______________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze

❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsumgebung**

Prüfgegenstand : **Raumgröße**

Arbeitsplatz :

Prüfdatum :

Vorschriften : ArbStättV §24 Abs.1, ZH 1/535, ZH 1/618

	Ja	Nein	i. A.
1. Fläche pro Bildschirmarbeitsplatz			
- in normalen Büros mindestens 10 m²	❑	❑	❑
- in Großraumbüros mindestens 15 m²	❑	❑	❑
2. Lichte Raumhöhe			
- Grundfläche ≤ 50 m² mindestens 2,50 m	❑	❑	❑
- Grundfläche > 50 m² mindestens 2,75 m	❑	❑	❑
- Grundfläche > 100 m² mindestens 3,00 m	❑	❑	❑
- Grundfläche >2000 m² mindestens 3,25 m	❑	❑	❑
3. Freiräume			
- Unverbaubare Fläche am Arbeitsplatz ≥ 1,5 m²	❑	❑	❑
- Freiraum hinter dem Arbeitsstuhl ≥ 1m	❑	❑	❑

Maßnahmen :	Frist :
____________________	__________
____________________	__________
____________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

<u>Prüfbereich</u> : **Arbeitsumgebung** <u>Prüfgegenstand</u> : **Beleuchtung**

<u>Arbeitsplatz</u> : <u>Prüfdatum</u> :

Vorschriften: DIN 66234 T 7, DIN 5034 T 1, DIN 5035 T 1+2+5, DIN 33400
DIN 5040 T 1+2, VDE 0108, ASA 7

	Ja	Nein	i. A.
1. Beleuchtungsstärke			
- Nennbeleuchtungsstärke mindestens 500 lx	❑	❑	❑
2. Leuchteneigenschaften			
- Flimmerfreie Beleuchtung	❑	❑	❑
- Einsatz tiefstrahlender Spiegelrasterleuchten	❑	❑	❑
- Neutralweiße oder warmweiße Lichtfarbe	❑	❑	❑
3. Leuchtenpositionierung			
- Leuchten parallel zur Hauptblickrichtung	❑	❑	❑
- Leuchtenreihen getrennt schaltbar	❑	❑	❑
- Keine Reflexion auf der Mattscheibe	❑	❑	❑
- Keine direkten Blendquellen im Gesichtsfeld	❑	❑	❑
- Tageslichteinfall durch Schutzeinrichtung reduzierbar	❑	❑	❑

Maßnahmen :	Frist :
______________________________	__________
______________________________	__________
______________________________	__________

<u>**Legende**</u> : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze

❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsumgebung** Prüfgegenstand : **Lärm**

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 33400, DIN 45641. DIN 45635 Bl.1+T 1+2, VDI 3729 Bl.1 VDE 2058 Bl.2+3, ArbStättV §15

	Ja	Nein	i. A
1.Schalldruckpegel im Raum			
- bei überwiegend geistiger Tätigkeit < 55 dB(A)	❑	❑	❑
- bei überwiegend mechanisierter Tätigkeit < 70 dB(A)	❑	❑	❑
- Keine unvermittelte Erhöhung	❑	❑	❑
2. Computer			
- Lüftergeräusch < 41 dB(A)	❑	❑	❑
- Laufwerkgeräusch < 42 dB(A)	❑	❑	❑
3. Drucker			
- Geräusch < 55 dB(A)	❑	❑	❑

Maßnahmen :	Frist :
______________________	__________
______________________	__________
______________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsmittel** Prüfgegenstand : **Arbeitstisch** (Teil 1)

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 4549, DIN 33402, DIN 66233, DIN 66234, VDI 2780
ZH 1/535, ZH 1/618

	Ja	Nein	i. A.
1. Höhe			
- nicht verstellbare Tische 720 mm	❑	❑	❑
- verstellbare Tische 680 mm bis 760 mm	❑	❑	❑
2. Breite			
- (k)ein Unterschrank min. 1200 mm besser 1600 mm	❑	❑	❑
- zwei Unterschränke min. 1600 mm	❑	❑	❑
3. Tiefe			
- Tischtiefe min. 800 mm besser 900 mm	❑	❑	❑
- Freiraum vor der Tastatur min. 50 mm besser 100 mm	❑	❑	❑
4. Arbeitsfläche			
- Vorhandene Freifläche min. 600 mm	❑	❑	❑
- Glanzgrad halbmatt bis seidenmatt	❑	❑	❑

Maßnahmen :	Frist :
______________________	__________
______________________	__________
______________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsmittel**

Prüfgegenstand : **Arbeitstisch** (Teil 2)

Arbeitsplatz :

Prüfdatum :

Vorschriften : DIN 4549, DIN 33402, DIN 66233, DIN 66234, VDI 2780
ZH 1/535, ZH 1/618

	Ja	Nein	i.A.
5. Beinraumhöhe bei nichteinstellbaren Tischen			
- an der Tischvorderkante min. 650 mm (besser 690 mm)	❑	❑	❑
- in 200 mm Tiefe min. 620 mm (besser 660 mm)	❑	❑	❑
- in 450 mm Tiefe min. 550 mm (besser 590 mm)	❑	❑	❑
- in 600 mm Tiefe min. 120 mm	❑	❑	❑
6. Beinraumbreite und -tiefe			
- Beinraumbreite durchgehend min. 580 mm	❑	❑	❑
- Beinraumtiefe min. 600 mm	❑	❑	❑
7. Gestaltung			
- Standsicherheit in jedem Betriebszustand	❑	❑	❑
- Keine Verletzungsgefahr durch Ecken, Griffe etc.	❑	❑	❑
- Flexible Anordnung der Arbeitsgeräte möglich	❑	❑	❑

Maßnahmen :	Frist :
______________________	__________
______________________	__________
______________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze

❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsmittel**

Prüfgegenstand : **Arbeitsstuhl** (Teil 1)

Arbeitsplatz :

Prüfdatum :

Vorschriften : DIN 4551, DIN 4552, DIN 68131, ZH 1/535, ZH 1/618

	Ja	Nein	i. A.
1. Sitzflächenabmessungen			
- Höhe für Bürodrehstühle 420 mm bis 530 mm	❑	❑	❑
- Höhe für Bürodrehsessel 430 mm bis 510 mm	❑	❑	❑
- Tiefe : nicht einstellbar 380 mm bis 420 mm	❑	❑	❑
- Tiefe : einstellbar 380 mm bis 440 mm	❑	❑	❑
- Breite : 400 mm bis 480 mm	❑	❑	❑
- Neigung : 2° nach vorn bis 12° nach hinten	❑	❑	❑
- Drehbare Sitzfläche	❑	❑	❑
2. Rückenlehnenmaße			
- Höhe nicht einstellbar min. 320 mm	❑	❑	❑
- Höhe einstellbar min. 220 mm	❑	❑	❑
- Breite 360 mm bis 480 mm	❑	❑	❑
- Neigung 80° bis 115° gegen die Sitzfläche	❑	❑	❑
- Befestigungspunkt 170 mm bis 230 mm über Sitzfläche	❑	❑	❑
- Rückstellkraft der Lehne dem Körpergewicht angepaßt	❑	❑	❑

Maßnahmen :	Frist :
______________________________	____________
______________________________	____________
______________________________	____________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsmittel** Prüfgegenstand : **Arbeitsstuhl** (Teil 2)

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 4551, DIN 4552, DIN 68131, ZH 1/535, ZH 1/618

	Ja	Nein	i. A.
3. Rollenausführungen			
- für harten Bodenbelag Rollentyp W	❑	❑	❑
- für weichen Bodenbelag Rollentyp H	❑	❑	❑
4. Armlehnen (bei Bedarf)			
- fest mit dem Stuhl verbunden	❑	❑	
- Länge min. 200 mm	❑	❑	
5. Sicherheit			
- Fünfarmiges Fußkreuz	❑	❑	❑
- Kippsicherheitsmaß min. 195 mm	❑	❑	
- Stolpermaß maximal 365 mm	❑	❑	
- Stoßdämpfung beim Hinsetzen	❑	❑	
6. Komfort			
- Dynamisches Sitzen realisierbar	❑	❑	❑
- Polster sind wasserdampf- und luftdurchlässig	❑	❑	❑

Maßnahmen :	Frist :
______________________	__________
______________________	__________
______________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsmittel** Prüfgegenstand : **Fußstütze**

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 4556, DIN 66234

	Ja	Nein	i. A.
1. Abmessungen			
- Höhenverstellung von 50 mm bis min. 110 mm	❑	❑	❑
- Tiefe min. 350 mm	❑	❑	❑
- Breite min. 450 mm	❑	❑	❑
- Neigungsverstellbereich von 5° bis 15°	❑	❑	❑
2. Fußsteuerung			
- in den hinteren Teil der Fußstütze integriert	❑	❑	❑
- Breite der Aussparung 200 mm bis 240 mm	❑	❑	❑
- Tiefe der Aussparung 118 mm bis 122 mm	❑	❑	❑
- Einbautiefe der Aussparung 18 mm bis 22 mm	❑	❑	❑
3. Sicherheit			
- Rutschfeste Fußplattenoberfläche	❑	❑	❑
- Rutschhemmender Stand	❑	❑	❑

Maßnahmen :	Frist :
______________________	__________
______________________	__________
______________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze

❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Arbeitsmittel**

Prüfgegenstand : **Vorlagehalter**

Arbeitsplatz :

Prüfdatum :

Vorschriften : DIN 66234 T 6, ZH 1/618

	Ja	Nein	i. A.
1. Fläche			
- entsprechend der Vorlage gewählt	❑	❑	❑
- Keine Leuchtdichtesprünge : Vorlage / Halter	❑	❑	
- Glanzgrad halbmatt bis seidenmatt	❑	❑	
2. Sehabstand			
- zwischen 500 mm und 800 mm	❑	❑	
3. Positionierung			
- Vorlagenhalter ist höhenverstellbar	❑	❑	❑
- Neigungsverstellbereich von 15° bis 75°	❑	❑	❑
- Flexible Aufstellung möglich	❑	❑	
4. Festigkeit			
- Konzept kann fixiert werden	❑	❑	❑
- Konzept kann bearbeitet werden	❑	❑	❑

Maßnahmen :	Frist :
______	______
______	______
______	______

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Hardware** Prüfgegenstand : **Bildschirm** (Teil1)

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 66234 T 1+2+6+9+10, DIN 8418, DIN 19060 T 1, ZH 1/618

	Ja	Nein	i. A.
1. Bildschirmoberfläche			
- Bildschirmdiagonale : 14" (Zoll) Textverarbeitung	❑	❑	❑
- Bildschirmdiagonale : 17" Graphikanwendungen	❑	❑	❑
- Bildschirmbreite : DIN A4	❑	❑	
- Bildschirmhöhe : min. 24 Zeilen à 80 Zeichen	❑	❑	
- Reflexionsarme Oberfläche (gerauht, geätzt)	❑	❑	❑
- Strahlungsarm	❑	❑	❑
- Kennzeichnung gem. Röntgenverordnung	❑	❑	❑
2. Bilddarstellung			
- Bildfolgefrequenz min. 65 Hz VGA-Graphikkarte	❑	❑	❑
- Bildschirmauflösung min. 640 x 480 VGA	❑	❑	
- Kontrast : Negativdarstellung 3:1 bis 15:1 (regelbar)	❑	❑	
- Kontrast : Positivdarstellung 6:1 bis 10:1 (regelbar)	❑	❑	

Maßnahmen :	Frist :

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze

❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Hardware**

Prüfgegenstand : **Bildschirm** (Teil 2)

Arbeitsplatz :

Prüfdatum :

Vorschriften : DIN 66234 T 1+2+6+9+10, DIN 8418, DIN 19060 T 1, ZH 1/618

	Ja	Nein	i. A.
3. Zeichendarstellung			
- Positivdarstellung	❑	❑	❑
- Scharfe Zeichendarstellung	❑	❑	❑
- Leuchtdichte zwischen 60 und 160 cd/m² einstellbar	❑	❑	
- Bunt : Schwarz/Weiß und max. sechs Farben (Purpur, Blau, Cyan, Grün, Gelb, Rot)	❑	❑	❑
- Unbunt : Weiß, Grau, Schwarz, Gelb, Orange, Grün	❑	❑	❑
4.Positionierung			
- Kein Kompaktgerät mit der Tastatur	❑	❑	❑
- Drehbares Bildschirmgerät	❑	❑	❑
- Vorlagenhalter ist höhenverstellbar	❑	❑	❑
- Neigungsverstellbereich von 15° bis 75°	❑	❑	❑
- Flexible Aufstellung möglich	❑	❑	

Maßnahmen :	Frist :
____________________	__________
____________________	__________
____________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Hardware** Prüfgegenstand : **Bildschirm** (Teil 3)

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 66234 T 1+2+6+9+10, DIN 8418, DIN 19060 T 1, ZH 1/618

	Ja	Nein	i. A.
5. Gehäuse			
- Neigungsverstellmöglichkeit um 5° nach vorn	❑	❑	❑
- Reflexionsgrad zwischen 20% und 50%	❑	❑	
- Glanzgrad halbmatt bis seidenmatt	❑	❑	❑
- Farbe entspricht der Umgebung	❑	❑	
- Vorsatzmöglichkeiten für Blenden und Filter	❑	❑	

Maßnahmen :	Frist :
___	___
___	___
___	___

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze

❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Hardware** | Prüfgegenstand : **Tastatur**

Arbeitsplatz : | Prüfdatum :

Vorschriften : DIN 33401, DIN 66234 T 5+6, DIN 2139, DIN 2137 T 2, DIN 2145

	Ja	Nein	i. A.
1. Tastaturmaße			
- Tastenabstand (Mitte) 18 mm bis 20 mm	❑	❑	❑
- Tastenweg 1 mm bis 5 mm	❑	❑	
- "C"-Tastenreihe weniger als 30 mm hoch	❑	❑	
- bei höheren Tastaturen : Handballenauflage vorhanden	❑	❑	❑
- Neigung geringer als 15°	❑	❑	❑
2. Tastenbetätigung			
- Tastenbelegung nach DIN 2137 T 2	❑	❑	❑
- Anschlagsbestätigung durch Druckpunkt	❑	❑	
- Anschlagsbestätigung durch Tonsignal (abschaltbar)	❑	❑	
3. Optische Gestaltung			
- Positivdarstellung auf der Tastatur	❑	❑	❑
- Glanzgrad halbmatt bis seidenmatt	❑	❑	❑
- Abgehobene Funktionstastatur	❑	❑	

Maßnahmen :	Frist :
______________________	__________
______________________	__________
______________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze

❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Hardware** Prüfgegenstand : **Drucker**

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 45641, VDE 0730

	Ja	Nein	i. A.
1. Beurteilungspegel			
- Druckergeräusch < 55 dB(A)	❑	❑	❑
- Keine unvermittelte Erhöhung	❑	❑	
2. Vibrationen			
- werden vom Drucker nicht verursacht	❑	❑	❑
3. Ausstattung			
- entspricht Anforderungen	❑	❑	
- Leistungsumfang entspricht Anforderungen	❑	❑	❑
- Benutzerorientiertes Handbuch vorhanden	❑	❑	❑
4. Toner			
- MAK-Werte werden eingehalten	❑	❑	

Maßnahmen :	Frist :
______________________	____________
______________________	____________
______________________	____________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Software** Prüfgegenstand : **Programme** (Teil 1)

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 66234 T 1-3+5+8, DIN 2140 T 1+2

	Ja	Nein	i. A.
1. Aufgabenangemessenheit			
- Minimale Restriktion	❑	❑	
- Zusammenhängende Informationsdarbietung	❑	❑	
- Anwenderspezifische Teilarbeitsbereiche	❑	❑	
- Formular in Maskendarstellung	❑	❑	
- Zusammenfassende Macrobildung	❑	❑	
2. Selbstbeschreibungsfähigkeit			
- Beschreibung auf Verlangen	❑	❑	
- Permanent-automatische Beschreibung	❑	❑	
3. Steuerbarkeit			
- frei wählbare Arbeitsgeschwindigkeit	❑	❑	
- Unterbrechung von fehlerhaften Arbeitsabläufen	❑	❑	
- Mehrstufige Sicherheitsabfragen	❑	❑	

Maßnahmen :	Frist :
______________________	__________
______________________	__________
______________________	__________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Prüfliste für Bildschirmarbeitsplätze
❑ Erstprüfung ❑ Wiederholungsprüfung

Prüfbereich : **Software** Prüfgegenstand : **Programme** (Teil 2)

Arbeitsplatz : Prüfdatum :

Vorschriften : DIN 66234 T 1-3+5+8, DIN 2140 T 1+2

	Ja	Nein	i. A.
4. Erwartungskonformität			
- Einheitliche Benutzeroberfläche	❑	❑	
- Einheitliche Bedeutung der Funktionstastatur	❑	❑	
- Kurze Antwortdauer	❑	❑	
- Anzeige bei längerer Antwortdauer	❑	❑	
- Dekodierungsfester auf dem Bildschirm	❑	❑	
5. Fehlerrobustheit			
- Angemessene Fehlermeldung	❑	❑	
- Hinweis auf Kapitel im Handbuch	❑	❑	

Maßnahmen :	Frist :
______________________________	______________
______________________________	______________
______________________________	______________

Legende : **Ja** : Anforderung erfüllt, **Nein** : Anforderung nicht erfüllt, **i.A.** : in Arbeit

Anhang 4-1

Teile des Bundesdatenschutzgesetzes

Bundesdatenschutzgesetz
(Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes)

Vom 20. Dezember 1990 (BGBl.I S. 2954, 2955)

****** Stand: 06/94 ******

Inhaltsübersicht

ERSTER ABSCHNITT

Allgemeine Bestimmungen

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch
1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
a) Bundesrecht ausführen oder
b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.

(3) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen:
1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§ 5 und 9.
2. Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§ 5, 9, 39 und 40.

Außerdem gelten für Dateien öffentlicher Stellen die Regelungen über die Verarbeitung und Nutzung personenbezogener Daten in Akten. Werden im Einzelfall personenbezogene Daten übermittelt,

gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt.

(4) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(5) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

§ 2 Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie derer Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Eine Datei ist
1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).
Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(3) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) Erheben ist das Beschaffen von Daten über den Betroffenen.

(5) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, dass
a) die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder
b) der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(6) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(7) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
(8) Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern lässt.
(9) Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieses Gesetzes personenbezogene Daten im Auftrag verarbeiten oder nutzen.

§ 4 Zulässigkeit der Datenverarbeitung und -nutzung

(1) Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.
(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.
(3) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 2 Satz 2 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6 Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen in einer Datei gespeichert, bei der mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, die speichernde Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die speichernde Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die speichernde Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

§ 7 Schadensersatz durch öffentliche Stellen

§ 8 Schadensersatz durch nicht-öffentliche Stellen

Macht ein Betroffener gegenüber einer nicht-öffentlichen Stelle einen Anspruch auf Schadensersatz wegen einer nach diesem Gesetz oder anderen Vorschriften über den Datenschutz unzulässigen oder unrichtigen automatisierten Datenverarbeitung geltend und ist streitig, ob der Schaden die Folge eines von der speichernden Stelle zu vertretenden Umstandes ist, so trifft die Beweislast die speichernde Stelle.

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 10 Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,
2. Datenempfänger,
3. Art der zu übermittelnden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn der für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesminister oder deren Vertreter zugestimmt haben.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offen stehen.

§ 11 Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6 bis 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1, Abs. 3 und 4 sowie § 44 Abs. 1 Nr. 2, 5, 6 und 7 und Abs. 2 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,
   b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personen-bezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig verarbeiten oder nutzen, die §§ 32, 36 bis 38.

Zweiter Abschnitt

DATENVERARBEITUNG DER ÖFFENTLICHEN STELLEN

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 12 Anwendungsbereich

§ 13 Datenerhebung

§ 14 Datenspeicherung, -veränderung und -nutzung

§ 15 Datenübermittlung an öffentliche Stellen

§ 16 Datenübermittlung an nicht-öffentliche Stellen

§ 17 Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes

§ 18 Durchführung des Datenschutzes in der Bundesverwaltung

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und
2. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten in Akten gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die speichernde Stelle bestimmt

das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§ 20 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten in Akten unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Personenbezogene Daten in Dateien sind zu löschen, wenn
1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit
1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten in Dateien sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten in Akten sind zu sperren, wenn die Behörde im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(6) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn
1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

(8) § 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§ 21 Anrufung des Bundesbeauftragten für den Datenschutz

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Dritter Unterabschnitt
Bundesbeauftragter für den Datenschutz

§ 22 Wahl des Bundesbeauftragten für den Datenschutz

§ 23 Rechtsstellung des Bundesbeauftragten für den Datenschutz

§ 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz

§ 25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz

§ 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz, Dateienregister

Dritter Abschnitt
Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 27 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder genutzt werden durch
1. nicht-öffentliche Stellen,
2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten in Akten, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer Datei entnommen worden sind.

§ 28 Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke

(1) Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig
1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,
2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt,

3. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung offensichtlich überwiegt,
4. wenn es im Interesse der speichernden Stelle zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

   Die Daten müssen nach Treu und Glauben und auf rechtmäßige Weise erhoben werden.

(2) Die Übermittlung oder Nutzung ist auch zulässig

1. a) soweit es zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist oder

   b) wenn es sich um listenmässig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf
   - eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
   - Berufs-, Branchen- oder Geschäftsbezeichnung,
   - Namen,
   - Titel,
   - akademische Grade,
   - Anschrift,
   - Geburtsjahr

   beschränken und

   kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. In den Fällen des Buchstabens b kann im allgemeinen davon ausgegangen werden, dass dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich
   - auf gesundheitliche Verhältnisse,
   - auf strafbare Handlungen,
   - auf Ordnungswidrigkeiten,
   - auf religiöse oder politische Anschauungen sowie
   - bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen, oder

2. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Widerspricht der Betroffene bei der speichernden Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Widerspricht der Betroffene beim Empfänger der nach Absatz 2 übermittelten Daten der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.

(4) Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen der Absätze 1 und 2 zulässig. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen.

§ 29 Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung

§ 30 Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form

§ 31 Besondere Zweckbindung

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 32 Meldepflichten

(1) Die Stellen, die personenbezogene Daten geschäftsmäßig
1. zum Zwecke der Übermittlung speichern,
2. zum Zwecke der anonymisierten Übermittlung speichern oder
3. im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, sowie ihre Zweigniederlassungen und unselbständigen

Zweigstellen haben die Aufnahme und Beendigung ihrer Tätigkeit der zuständigen Aufsichtsbehörde innerhalb eines Monats mitzuteilen.

(2) Bei der Anmeldung sind folgende Angaben für das bei der Aufsichtsbehörde geführt Register mitzuteilen:
1. Name oder Firma der Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift,
4. Geschäftszwecke der Stelle und der Datenverarbeitung,
5. Name des Beauftragten für den Datenschutz,
6. allgemeine Beschreibung der Art der gespeicherten personenbezogenen Daten. Im Falle des Absatzes 1 Nr. 3 ist diese Angabe nicht erforderlich.

(3) Bei der Anmeldung sind außerdem folgende Angaben mitzuteilen, die nicht in das Register aufgenommen werden:
1. Art der eingesetzten Datenverarbeitungsanlagen,
2. bei regelmäßiger Übermittlung personenbezogener Daten Empfänger und Art der übermittelten Daten.

(4) Absatz 1 gilt für die Änderung der nach Absätzen 2 und 3 mitgeteilten Angaben entsprechend.

(5) Die Aufsichtsbehörde kann im Einzelfall festlegen, welche Angaben nach Absatz 2 Nr. 4 und 6, Absatz 3 und Absatz 4 mitgeteilt werden müssen. Der mit den Mitteilungen verbundene Aufwand muss in einem angemessenen Verhältnis zu ihrer Bedeutung für die Überwachung durch die Aufsichtsbehörde stehen.

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 33 Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke gespeichert, ist der Betroffene von der Speicherung und der Art der Daten zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen,
3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,
4. die zuständige öffentliche Stelle gegenüber der speichernden Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
5. die Daten in einer Datei gespeichert werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht wird,
6. die Daten für eigene Zwecke gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind oder
   b) die Benachrichtigung die Geschäftszwecke der speichernden Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder
7. die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und
   a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder
   b) es sich um listenmässig oder sonst zusammengefasste Daten handelt (§ 29 Abs. 2 Nr. 1 Buchstabe b).

§ 34 Auskunft an den Betroffenen

(1) Der Betroffene kann Auskunft verlangen über
1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,
2. den Zweck der Speicherung und
3. Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden.

Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten

geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. In diesem Falle ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.

(2) Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie nicht in einer Datei gespeichert sind. Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. § 38 Abs. 1 ist mit der Maßgabe anzuwenden, dass die Aufsichtsbehörde im Einzelfall die Einhaltung von Satz 1 überprüft, wenn der Betroffene begründet darlegt, dass die Auskunft nicht oder nicht richtig erteilt worden ist.

(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Nr. 2 bis 6 nicht zu benachrichtigen ist.

(5) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, dass die Daten zu berichtigen oder unter der Voraussetzung des § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(6) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Er ist hierauf in geeigneter Weise hinzuweisen.

§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,

2. es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen handelt und ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden und eine Prüfung am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, dass eine länger währende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit
1. im Falle des Absatzes 2 Nr. 3 oder 4 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(6) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung der schutzwürdigen Interessen des Betroffenen erforderlich ist.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn
1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden

Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Dritter Unterabschnitt
Beauftragter für den Datenschutz, Aufsichtsbehörde

§ 36 Bestellung eines Beauftragten für den Datenschutz

(1) Die nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten und damit in der Regel mindestens fünf Arbeitnehmer ständig beschäftigen, haben spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit einen Beauftragten für den Datenschutz schriftlich zu bestellen. Das gleiche gilt, wenn personenbezogene Daten auf andere Weise verarbeitet werden
und damit in der Regel mindestens zwanzig Arbeitnehmer ständig beschäftigt sind.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

(3) Der Beauftragte für den Datenschutz ist dem Inhaber, dem Vorstand, dem Geschäftsführer oder dem sonstigen gesetzlich oder nach der Verfassung des Unternehmens berufenen Leiter unmittelbar zu unterstellen. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann nur auf Verlangen der Aufsichtsbehörde oder in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(5) Die nicht-öffentliche Stelle hat den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

§ 37 Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz hat die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Zu diesem Zweck kann er sich in Zweifelsfällen an die Aufsichtsbehörde wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenden besonderen Erfordernisse für den Datenschutz, vertraut zu machen,
3. bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken.

(2) Dem Beauftragten ist von der nicht-öffentlichen Stelle eine Übersicht zur Verfügung zu stellen über

1. eingesetzte Datenverarbeitungsanlagen,
2. Bezeichnung und Art der Dateien,
3. Art der gespeicherten Daten,
4. Geschäftszwecke, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
5. deren regelmäßige Empfänger,
6. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.

(3) Absatz 2 Nr. 2 bis 6 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

§ 38 Aufsichtsbehörde

Vierter Abschnitt
Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

§ 41 Verarbeitung und Nutzung personenbezogener Daten durch die Medien

§ 42 Datenschutzbeauftragte der Rundfunkanstalten des Bundesrechts

Fünfter Abschnitt
Schlußvorschriften

§ 43 Strafvorschriften

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,
   1. speichert, verändert oder übermittelt,
   2. zum Abruf mittels automatisierten Verfahrens bereithält oder
   3. abruft oder sich oder einem anderen aus Dateien verschafft,

   wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer
   1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,
   2. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 4 Satz 1, auch in Verbindung mit § 29 Abs. 3, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
   3. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 3 Satz 3 die in § 40 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(4) Die Tat wird nur auf Antrag verfolgt.

§ 44 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
2. entgegen § 32 Abs. 1, auch in Verbindung mit Absatz 4, eine Meldung nicht oder nicht rechtzeitig erstattet oder entgegen § 32 Abs. 2, auch in Verbindung mit Absatz 4, bei einer solchen Meldung die erforderlichen Angaben nicht, nicht richtig oder nicht vollständig mitteilt,
3. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
4. entgegen § 35 Abs. 5 Satz 3 Daten ohne Gegendarstellung übermittelt,
5. entgegen § 36 Abs. 1 einen Beauftragten für den Datenschutz nicht oder nicht rechtzeitig bestellt,
6. entgegen § 38 Abs. 3 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 38 Abs. 4 Satz 4 den Zutritt zu den Grundstücken oder Geschäftsräumen oder die Vornahme von Prüfungen oder Besichtigungen oder die Einsicht in geschäftliche Unterlagen nicht duldet, oder
7. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),
5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Anhang 4-2 Tabelle 4-1

Sicherungsmaßnahmen nach Datenklassen

Beschreibung der Datenstufung, auf die sich die Tabelle bezieht

- Stufe A: personenbezogene Daten, deren Missbrauch keine besondere Beeinträchtigung erwarten lässt, z.B.
  * Adressangaben (Name, Anschrift, Tel.-Nr.),
  * Berufs-, Branchen- oder Geschäftsbezeichnungen;

- Stufe B: personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen kann, z.B.
  * Daten über Mietverhältnisse,
  * Daten über Geschäftsbeziehungen;

- Stufe C: personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen kann, bzw. die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, insbesondere die Daten, die in § 28 Absatz 2 Nr.1 BDSG aufgeführt sind, die sich auf
  * gesundheitliche Verhältnisse,
  * strafbare Handlungen,
  * Ordnungswidrigkeiten,
  * religiöse oder politische Anschauungen,
  * arbeitsrechtliche Rechtsverhältnisse

  beziehen;

Einführung zu Tabelle 4-1

Sicherungsmaßnahmen für Stufe A

Datenträgerkontrolle:
- Geschützte Aufbewahrung der Datensicherungsträger

Benutzerkontrolle:
- Paßwortabfrage und -verwaltung (Begrenzung der Anmeldeversuche, begrenzte Gültigkeitsdauer, Mindestlänge, Identitätsvergleich mit abgelaufenen Paßwörtern)
- Vermeidung mehrerer Netzanmeldungen unter einer Benutzerkennung
- Nutzung des File-Servers ausschließlich im dedizierten Betrieb
- Begrenzung der Netzverwaltung auf einen speziellen Arbeitsplatzrechner durch explizites Definieren von Netzwerkadressen

Zugriffskontrolle:
- Sicherung der Server-Platte vor unberechtigtem Zugriff durch spezielles Festplattenformat sowie geeigneten Bootschutz
- Benutzerspezifische, abgestufte Rechteverwaltung auf Unterverzeichnis- und Dateiebene

Übermittlungskontrolle:
- Lese-/Schreib-Schutz der lokalen Festplatte gegenüber anderen Netzanwendern

Transportkontrolle:
- Verwendung von abgeschirmten Kabeln zwecks höherer Abhörsicherheit
- Vermeidung offenliegender Netz-Steckdosen, um Anschluß netzfremder Personalcomputer zu erschweren

Tabelle 4-1 Sicherungsmaßnahmen nach Datenklassen I

Sicherungsmaßnahmen für Stufe B

Datenträgerkontrolle:
- menügesteuerte Datensicherung durch den Netzverwalter
- Verschlüsselung der Datensicherungsträger
- Aufbewahrung der Datensicherungsträger in Sicherheitsschränken
- Sicherung der seriellen Schnittstelle vor unberechtigtem Zugriff

Benutzerkontrolle:
- Paßwortabfrage und -verwaltung (Begrenzung der Anmeldeversuche, begrenzte Gültigkeitsdauer, Mindestlänge, Identitätsvergleich mit abgelaufenen Paßwörtern)
- Einsatz geeigneter Verschlüsselungsverfahren zur Übertragung von Paßwörtern über das Netz
- Vermeidung mehrerer Netzanmeldungen unter einer Benutzerkennung
- Nutzung des File-Servers ausschließlich im dedizierten Betrieb
- Begrenzung der Netzverwaltung auf einen speziellen Arbeitsplatzrechner durch explizites Definieren von Netzwerkadressen
- Gehäuseschloss oder Verplomben sämtlicher Geräte

Zugriffskontrolle:
- Sicherung der Server-Platte vor unberechtigtem Zugriff durch spezielles Festplattenformat sowie geeigneten Bootschutz
- Benutzerspezifische, abgestufte Rechteverwaltung auf Unterverzeichnis- und Dateiebene
- Bindung der Zugriffsberechtigung an spezielle Arbeits-platzrechner
- kein Betriebssystemzugriff auf dem Arbeitsplatzrechner, ausschließliche Menüsteuerung im Netzwerk
- Bildschirmverdunkelung auf dem Arbeitsplatzrechner durch den Benutzer bei Arbeitsunterbrechung, Weiterarbeit erst nach erneuter Paßwort-Eingabe

Tabelle 4-1 Sicherungsmaßnahmen nach Datenklassen II

Noch Sicherungsmaßnahmen für Stufe B

Übermittlungskontrolle:
- Lese-/Schreib-Schutz der lokalen Festplatte gegenüber anderen Netzanwendern
- Trennung von lokaler und Netzanwendung durch Schreibschutz auf der lokalen Festplatte

Eingabekontrolle:
- Protokollierung sämtlicher Aktivitäten auf dem File-Server einschließlich gescheiterter Zugriffsversuche
- Protokollierung der Netzverwaltung
  * Veränderung von Zugriffsrechten
  * Lese- und Schreibzugriff auf Dateien mit personenbezogenen Daten
  * Aufruf von Programmen
- Auswertung der Protokolle durch eine Person, die keine Netzverwaltung wahrnimmt

Transportkontrolle:
- Verwendung von abgeschirmten Kabeln zwecks höherer Abhörsicherheit
- Vermeidung offenliegender Netz-Steckdosen, um Anschluß netzfremder Personalcomputer zu erschweren

Tabelle 4-1 Sicherungsmaßnahmen nach Datenklassen III

Sicherungsmaßnahmen für Stufe C

Datenträgerkontrolle:
- menügesteuerte Datensicherung durch den Netzverwalter
- Verschlüsselung der Datensicherungsträger nach dem DES-Verfahren
- Aufbewahrung der Datensicherungsträger im Tresor
- Sicherung der seriellen Schnittstelle vor unberechtigtem Zugriff

Benutzerkontrolle:
- Paßwortabfrage und -verwaltung (Begrenzung der Anmeldeversuche, begrenzte Gültigkeitsdauer, Mindestlänge, Identitätsvergleich mit abgelaufenen Paßwörtern)
- einwegverschlüsselte Paßwörter
- Einsatz geeigneter Verschlüsselungsverfahren zur Übertragung von Paßwörtern über das Netz
- Vermeidung mehrerer Netzanmeldungen unter einer Benutzerkennung
- Nutzung des File-Servers ausschließlich im dedizierten Betrieb
- Begrenzung der Netzverwaltung auf einen speziellen Arbeitsplatzrechner durch explizites Definieren von Netzwerkadressen
- Gehäuseschloß oder Verplomben sämtlicher Geräte

Zugriffskontrolle:
- Sicherung der Server-Platte vor unberechtigtem Zugriff durch spezielles Festplattenformat sowie geeigneten Bootschutz
- Benutzerspezifische, abgestufte Rechteverwaltung auf Unterverzeichnis- und Dateiebene
- Netzverwaltung nach dem Vier-Augen-Prinzip (Vier-Augen-Prinzip kann über zwei Paßwörter, die jeweils dem Netzverwalter und einer weiteren Person bekannt sind, umgesetzt werden)
- Bindung der Zugriffsberechtigung an spezielle Arbeitsplatzrechner

Tabelle 4-1 Sicherungsmaßnahmen nach Datenklassen IV

Noch Sicherungsmaßnahmen für Stufe C

- kein Betriebssystemzugriff auf dem Arbeitsplatzrechner, ausschließliche Menüsteuerung im Netzwerk
- Bildschirmverdunkelung auf dem Arbeitsplatzrechner durch den Benutzer bei Arbeitsunterbrechung, Weiterarbeit erst nach erneuter Paßwort-Eingabe
- Verschlüsselung von Dateien mit sehr sensiblen personenbezogenen Daten nach dem DES-Verfahren
- physikalisches Löschen personenbezogener Daten

Übermittlungskontrolle:
- Lese-/Schreib-Schutz der lokalen Festplatte gegenüber anderen Netzanwendern
- Trennung von lokaler und Netzanwendung durch Schreibschutz auf der lokalen Festplatte
- Verschlüsselung der übertragenen Daten

Eingabekontrolle:
- Protokollierung sämtlicher Aktivitäten auf dem File-Server einschließlich gescheiterter Zugriffsversuche
- Protokollierung der Netzverwaltung
  * Veränderung von Zugriffsrechten
  * Lese- und Schreibzugriff auf Dateien mit personenbezogenen Daten
  * Aufruf von Programmen
- Auswertung der Protokolle durch eine Person, die keine Netzverwaltung wahrnimmt

Transportkontrolle:
- Verwendung von abgeschirmten Kabeln zwecks höherer Abhörsicherheit
- Vermeidung offenliegender Netz-Steckdosen, um Anschluss netzfremder Personalcomputer zu erschweren

Tabelle 4-1 Sicherungsmaßnahmen nach Datenklassen V

Anhang 4-3

Mögliche Schutz-/Sicherheitssysteme beim Einsatz von Personalcomputern /Brandenburg/

Die z. Z. auf dem Markt befindlichen Betriebssysteme für PC und Netzwerke haben den Datenschutz und die Datensicherheit unterschiedlich realisiert. Für Verarbeitung von Daten, die eine gewisse Sensitivitätsstufe haben, sind die betriebssystemeigenen Schutzvorkehrungen in der Regel nicht ausreichend, denn sie können leicht umgangen werden.
Für die einzelnen Betriebssysteme ist eine Reihe von Zusatzprodukten verschiedener Hersteller erhältlich, die deren Schutzvorkehrungen ergänzen. Diese Zusatzprodukte bestehen teilweise aus Software, teilweise aus einer Kombination von Hard- und Software.
Die Entscheidung über Einsatz und Auswahl solcher Produkte kann nur unter Berücksichtigung der betrieblichen Gegebenheiten erfolgen. Der gewünschte Leistungsumfang, die Struktur der mit dem PC zu erledigenden Aufgaben und das organisatorische Umfeld sind dabei wichtige Faktoren.

Sicherheitskomponenten können z. B. sein:
1. Benutzerverwaltung
- Verwaltung mehrerer Benutzer
- Verteilung der Funktionen auf verschiedene Personen mit entsprechender Menüführung

2. Benutzerpaßwörter
- Paßwortwechsel durch den Benutzer
- begrenzte Gültigkeitsdauer
- Paßwortwechsel und Eingabe ohne Anzeige
- Mindestlänge einstellbar
- verschlüsselte Speicherung der Paßwörter
- Begrenzung erfolgloser Login-Versuche

3. Einschränkungen auf Benutzerebene
- Sperrung der Diskettenlaufwerke
- Beschränkung auf Lesen bzw. Schreiben von Disketten
- Benutzerkennung mit Benutzerprofil
- Zugriffsregelung für Dateien, Datensätze und Datenfelder
- Zugriffsregelung für Programme und einzelne Systemkommandos

- Beschränkung des Festplattenzugriffs auf bestimmte Bereiche und/oder Verzeichnisse
- Ausschluß der Benutzung bestimmter Befehls- oder Dateinamen

4. Festplatte/Diskette
- Festplattenpasswort
- besonderer Schlüssel oder Paßwort für einzelne Plattenbereiche
- kein Systemstart von Diskette
- Verschlüsselung von Disketten
- Verschlüsselung der Festplatte oder von einzelnen Dateien
- Virensuchprogramme

5. Protokollierung
- Login, Logout
- erfolglose Login-Versuche
- eventuell Überschreitung der Berechtigung
- Programmaufrufe
- Dateien (eröffnen, anlegen, lesen, schreiben, löschen)
- Auswertungsmöglichkeiten der Protokolldatei
- bei Personenverschiedenheit von Bediener und Veranlasser: Protokol-lierung des Veranlassers

6. Tastatur, Bildschirm
- erneute Eingabe des Paßwortes nach Ablauf einer bestimmten Zeitspanne ohne Benutzeraktivitäten
- Pausenschaltung (Dunkelschaltung des Bildschirms) bei kurzfristigen Unterbrechungen

Anhang 6-1 Tabelle 6.2

Vorgehensweise bei der Beschaffung von EDV nach Gerken

1. Voruntersuchung

1.1 Voruntersuchung durchführen
1.1.1 Ermittlung der Probleme und Wünsche
1.1.2 Zielvorstellungen
1.1.2.1 Zwingende Zielvorstellungen
1.1.2.2 Wünschenswerte Zielvorstellungen
1.1.3 Mögliche Anwender
1.1.4 Vorstellungen der Anwender/Auftraggeber
1.1.5 Abschätzung der Mengengerüste (Aufgabenhäufigkeit/Datenvolumen)
1.1.6 Erwartete Verbesserungen
1.1.7 Gewünschter Fertigstellungstermin
1.1.8 Beziehungen zu bestehenden EDV-Systemen
1.1.9 Beziehungen zu manuell erledigten Aufgaben
1.1.10 Möglichkeiten zur Verwendung vorhandener Lösungen

1.2 Projektziele festlegen
1.2.1 Ziele ausformulieren
1.2.2 Ziele ordnen
1.2.3 Prioritäten festlegen

1.3 Vorgehensplan erstellen
1.3.1 Phasenplanung für den Projektverlauf
1.3.2 Terminplanung
1.3.3 Kostenplanung
1.3.4 Personal-Einsatzplanung

1.4 Festlegen der Entwicklungsrichtlinien
1.4.1 Vorgabe der anzuwendenden Methoden und Techniken und die Verwendung und die Verwendung von Software-Tools bei Analyse, Entwurf, Implementierung und Test.
1.4.2 Zu berücksichtigende Normen und Tests
1.4.3 Dokumentationsrichtlinien für den Entwicklungsprozess und das Entwicklungsprojekt mit allen seinen Zwischenergebnissen.

1.5 Rechtfertigung des Projektes

1.5.1 Klärung der Frage von Eigenentwicklungen
1.5.2 Beschaffung zusätzlicher Hard/Software
1.5.3 Personalbedarf
1.5.4 Zeitbedarf
1.5.5 Kosten/Nutzen-Analyse
1.5.6 Projektantrag

2 Analyse

2.1 Ist-Aufnahme

2.1.1 Aufgaben (des Projektgegenstandes)
2.1.1.1 Art der Aufgaben
2.1.1.2 Abwicklung der Aufgaben (bisher)
2.1.2 Ziel der Aufgabenerfüllung
2.1.3 Vorhandene Arbeitsanweisungen, Unterlagen, Formulare etc.
2.1.4 Vorhandene Karteien, bzw. Dateien
2.1.5 Mengengerüst der Daten
2.1.6 Kommunikationsstruktur
2.1.7 Häufigkeit des Aufgabenanfalls
2.1.8 Zeitliche Anforderungen an die Aufgabe
2.1.9 Aufgabenträger (personell und sachlich)
2.1.10 Hilfsmittel, Formulare
2.1.11 Sicherheitsanforderungen, insbesondere Datensicherheit
2.1.12 Beziehung der jeweiligen Aufgabe zu anderen
2.1.13 Arbeitsort
2.1.14 Impuls zur Aufgabenerfüllung
2.1.15 Schwachstellen der bisherigen Lösungen
2.1.16 Verbesserungsmöglichkeiten

2.2 Schwachstellenanalyse

2.2.1 Aus Anwendersicht
2.2.1.1 Umständliche Abläufe
2.2.1.2 Ungeeignete technische Hilfsmittel
2.2.1.3 Doppelerfassung von Daten
2.2.1.4 Quantitative und qualitative Mängel der Ausgabedaten
2.2.1.5 Verzögerungen im Ablauf

2.2.2 Aus Management-Sicht
2.2.2.1 Fehlende Informationen
2.2.2.2 Überflüssige Informationen
2.2.2.3 Zu hohe Kosten

2.3 Anforderungskatalog (Pflichtenheft)
2.3.1 Funktionale Anforderungen
2.3.1.1 Beschreibung der Systemfunktionen (notwendig/wünschenswert)
2.3.1.2 Beschreibung der Daten
- Eingabe, - Ausgabe
- Mengengerüst
- Wertebereiche
- Plausibilitätsprüfungen

2.3.1.3 Normalfall-Sonderfall-Betrachtungen
2.3.2 Anforderungen an das EDV-System
2.3.2.1 Benutzerfreundlichkeit
2.3.2.2 Kompatibilität und Portabilität
2.3.2.3 Organisatorische Abwicklung
2.3.2.4 Technische Anforderungen
2.3.2.5 Systemsicherheit und Datenschutz
2.3.2.6 Antwort-Zeit-Verhalten
2.3.2.7 Wartung und Betreuung des implementierten Systems
2.3.3 Gegebene Randbedingungen
2.3.3.1 Anforderungen an die Systemeinführung
2.3.3.2 Vorgegebene Hardware-Konfiguration
2.3.3.3 Gegebene System- und systemnahe Software
2.3.3.4 Schnittstellen zu Anwendersoftware (Text; Graphikprogramme)
2.3.3.5 Vorhandene Programme, die in das System zu integrieren sind

2.4 Überprüfen des Anforderungskataloges aus 2.3 nach
- Prinzipieller Erfüllbarkeit
- Technischer Realisierbarkeit
- Wirtschaftlicher Vertretbarkeit
- Möglicher Akzeptanz

3 Lösungskonzepte

3.1 Idealkonzept

3.2 Grobkonzept

3.2.1 Funktionsbeschreibung
3.2.2 Schnittstellenbeschreibung
3.2.3 Notwendige Hardware-Konfiguration
3.2.4 Notwendige System- und Standard-Software
3.2.5 Datensicherheit und Datenschutzmaßnahmen
3.2.6 Notbetrieb
3.2.7 Entwicklungskosten und -Dauer
3.2.8 Datenübernahme von vorhandenen Datenträgern in das neue EDV- System
3.2.9 Deckungsgrad mit dem Anforderungskatalog
3.2.10 Derzeit nicht erfüllbare Forderungen inkl. Begründung

3.3 Präsentation (Diskussion der Konzepte)

unter den Aspekten
- Risiko - Technik - Know How
- Kosten - Nutzen

4 Systementwurf/Beschaffung

4.1 Vertiefung der Ist-Aufnahme (wo notwendig)

4.2 Systemstrukturierung (Bei Eigenprogrammierung)

4.2.1 Detaillierte Funktionsspezifikationen
4.2.2 Entwurf der Dialog- und Funktionsabläufe
4.2.3 Logische Datenanalyse
4.2.4 Zusammenfassung von Funktionen zu Programmen
4.2.5 Schnittstellen zwischen Programmen definieren
4.2.6 Eine graphische Systemübersicht erstellen (auch b. Kauf günstig)

4.3 Systemkonfigurierung
4.3.1 Festlegung der notwendigen Systemsoftware
4.3.2 Festlegung bereits vorhandener und verwendbarer Anwendersoftware
4.3.3 Festlegung neu zu programmierender Software
4.3.4 Festlegung zu beschaffender Standardsoftware
4.3.5 Bestimmung der Hardware-Konfiguration
4.3.6 Eingliederung in das organisatorische Umfeld

4.4 Systemtestplan erstellen
4.5 Diskussion der Punkte 4.1 -4.4 z.B. unter Kosten-Nutzen, Realisierbarkeit, Akzeptanz etc.

5 Detail-Entwurf

5.1 Datenspezifikation (nur bei Eigenprogrammierung nötig)
5.2 Schnittstellenspezifikation (b. Eigenprogram. notwendig)
5.3 Programmspezifikation (bei Eigenprogram. notwendig)
5.4 Testspezifikation (nur bei Eigenprogrammierung notwendig)

6 Implementierung

6.1 Generierung der Datenbasis
6.2 Generierung der Masken
6.3 Codierung- Generierung der Programme
6.4 Erzeugung von Testdaten
6.5 Programmtest

oder statt 5 und 6: Testen von zu kaufender Software anhand des mittels der Punkte 2 und 4 erstellten Pflichtenheftes

7 Integration
7.1 Softwareanpassungen
7.2 Bedienungshandbücher
7.3 Systemtest

8 Installation und Einführung

Anhang 6-2 Tabelle 6.3

Aufgaben der Fachkräfte für Arbeitssicherheit /Gra/

1. Den Unternehmer, die Geschäftsführung, den Behördenleiter und die anderen für die Arbeitssicherheit und die Unfallverhütung verantwortlichen Führungskräfte unterstützen durch

1-1 Sicherheitstechnisches Beraten beim
- Planen, Einrichten, Nutzen und Instandhalten von
-- Grundstücken
-- Gebäuden
- Räume (z.B. Betriebsräume, Büroräume, Sozialräume, Sanitärräume)
- andere Gebäudeteile (z.B. Rampen, Treppen)
-- andere baulichen Anlagen (z.B. Schranken, Schutzgeländer)

- Planen, Errichten, Beschaffen, Auswählen, Erproben und Instandhalten von
-- technischen Einrichtungen
- Fahrzeugtechnische Einrichtungen (z.B. Kraftfahrzeuge, Flugförderzeuge)
- Haustechnische Einrichtungen (z.B. elektrische Versorgungsanlagen, lüftungstechnische Geräte und Anlagen)
- Betriebstechnische Einrichtungen (z.B. Fördertechnische Einrichtungen, Büromaschinen und Geräte)
- Fernmeldetechnische Einrichtungen (z.B. Vermittlungsanlagen)
-- Arbeitsstoffen
- Gefahrenstoffe
- Andere Arbeitsstoffe

- Beschaffen, Auswählen und Erproben von Körperschutzmitteln

- Einführen von Arbeitsverfahren

- Ergonomisches Gestalten von
-- Arbeitsabläufen
-- Arbeitsmitteln
-- Arbeitsplätzen
-- Arbeitsbereichen
-- Arbeitsumgebung

- Erstellen von unternehmens-/verwaltungsinternen Dienst- und Arbeitsvorschriften in Form von
-- Arbeitsanweisungen
-- Richtlinien
-- Merkblättern

1-2 Sicherheitstechnisches Überprüfen von
- Grundstücken, Gebäuden, anderen baulichen Anlagen und technischen Einrichtungen
-- vor der erstmaligen Inbetriebnahme
-- bei Wiederinbetriebnahme und Änderungen
-- regelmäßig
-- nach besonderem Programm

- Persönlichen Schutzausrüstungen

- Arbeitsverfahren
-- vor der erstmaligen Einführung
-- bei Änderungen

1-3 Beobachten der Durchführung des Arbeitsschutzes und der Unfallverhütung
- regelmäßiges Begehen der Arbeitsstätten
- Achten auf das Benutzen der vorgeschriebenen Körperschutzmittel
- Auswerten von Schadensmeldungen
- Analysieren von Beinahe-Unfällen
- Auswerten der Unfallstatistiken
- Kontrollieren der fristgerechten Einhaltung der in Gesetzen, Verordnungen und Unfallverhütungsvorschriften usw. vorgeschriebenen Sachverständigen- und Sachkundigenprüfungen
- Vorbeugendes Durchführen von Gefährdungsanalysen
- Ermitteln der Ursachen von Dienst- und Arbeitsunfällen durch
-- Auswerten der einzelnen Unfallanzeigen und -vermerke
-- unfallbezogene Gefährdungsanalysen

1-4 Mitteilen der beim Beobachten festgestellten Mängel

1-5 Vorschlagen von
- Maßnahmen zur Beseitigung der anläßlich von
-- Betriebsbegehungen festgestellten Mängel
-- Gefährdungsanalysen festgestellten Mängel
-- beim sonstigen Beobachten festgestellten Mängel
-- beim sonstigen Beobachten festgestellten Mängel
- Verwaltungs- und betriebsspezifischen Arbeitsschutzprogrammen

1-6 Hinwirken auf sicherheitsgerechtes Verhalten der Beschäftigten durch Motivieren und Belehren im Rahmen von
- Einzelgesprächen
- Dienstbesprechungen
- Betriebs-/Personalversammlungen
- sonstigen aktuellen Anlässen

1-7 Fördern des Sicherheitsbewusstseins der Beschäftigten durch
- Beschaffen und Verteilen von außerbetrieblich erstelltem Informationsmaterial
- eigenes Erstellen und Verteilen von betriebs-/ verwaltungsspezifisch erstellten Informationsmaterial
- Aktionen der Arbeitssicherheit in Form von
-- Unfallverhütungsaktionen
-- anderen Werbeaktionen
- Informieren der neu eingestellten Beschäftigten über
-- betriebsbedingten Fragen des Arbeitsschutzes und der Unfallverhütung
-- die besonderen Verwaltungs- und betriebsspezifischen Gefahren und deren Abwendung
-- die innerbetriebliche Sicherheitsorganisation

1-8 Mitwirkung bei der Schulung und Betreuung der Sicherheitsbeauftragten

2 Zusammenarbeiten mit

2-1 dem Betriebs-/ Personalrat durch
- Informieren über wichtige Angelegenheiten des Arbeitsschutzes und der Unfallverhütung
- Mitteilen der an den Behördenleiter oder Unternehmer in der Verwaltung direkt gerichteten sicherheitstechnischen Vorschläge
- Beraten über die Angelegenheiten des Arbeitsschutzes und der Unfallverhütung

2-2 dem Betriebsarzt durch
- gemeinsame Betriebsbegehungen
- Erörtern von arbeitsmedizinischen und sicherheitstechnischen Lösungen

2-3 außerbetrieblichen Stellen des Arbeitsschutzes
- Unfallversicherungsträger
- Gewerbeaufsicht
- Überwachungsämter und -vereine
- andere Institute

3 Im Arbeitsschutzausschuss mitwirken

4 Sonstige Aufgaben wahrnehmen durch

4-1 Mitwirken bei außerbetrieblich veranlassten ergonomischen und sicherheitstechnischen Untersuchungen und Prüfungen
- der Unfallversicherungsträger (technische Aufsicht)
- der Gewerbeaufsichtsämter (Gewerbeaufsichtsamt)
- der technischen Überwachungsämter, -vereine, der Eigenüberwachung
- anderer Institute

4-2 Mitwirken beim Bestellen von Sicherheitsbeauftragten
4-3 Stellung nehmen zur Auslegung von Vorschriften des Arbeitsschutzes und der Unfallverhütung
4-4 Mitwirken bei Besprechungen mit außerhalb der Verwaltung und des Betriebes stehenden Stellen über sicherheitstechnische Fragen
4-5 Sicherheitstechnische Begutachtung von arbeitsschutzbezogenen Verbesserungsmöglichkeiten

Anhang 7-1

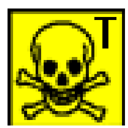
Beispiele für eine Betriebsanweisung

Universität Regensburg	***Betriebsanweisung***	***Nr.:***
Ort	***gem. § 20 GefStoffV***	***e-038***

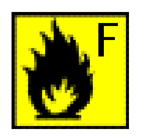
Gefahrstoff:...***Benzol***

C6 H6, CAS-Nr. 71-43-2
Farblose Flüssigkeit mit typischem aromatischen Geruch

Gefahr für Mensch und Umwelt



Kann Krebs erzeugen.
Giftig: Gefahr ernster Gesundheitsschäden bei längerer Exposition durch Einatmen, Berührung mit der Haut und durch Verschlucken



Leichtentzündlich
Elektrostatisch aufladbar

Gefährliche Reaktionen
Stark wassergefährdend (WGK 3)

Schutzmaßnahmen und Verhaltensregeln
Bei Unfall oder Unwohlsein sofort Arzt hinzuziehen und diese Betriebsanweisung vorzeigen.
Exposition vermeiden – vor Gebrauch besondere Anweisungen einholen.
Immer im Abzug arbeiten.
Vorsicht im Kontakt mit Stoffen, die gefährliche Reaktionen verursachen.
Bei Gefahr des Hautkontaktes Schutzhandschuhe benutzen.
Beschäftigungserlaubnis für Jugendliche über 16 Jahre nur, wenn das Ausbildungsziel den Umgang notwendig macht und eine fachkundige Aufsicht gewährleistet ist.

Verhalten im Gefahrfall
Stoff-freisetzung: Kleine Spritzer mit saugfähigem Papier, größere Mengen nur unter umgebungsluftunabhängigem Atemschutz mit Absorptionsmaterial (Vermiculit) aufnehmen. Ggf. Labor räumen!

Brandfall: CO_2-, Pulver-Löscher oder Wasser im Sprühstrahl einsetzen und Druckknopfmelder betätigen! Technische Zentrale informieren 33 33. Feuerwehr auf giftige Dämpfe aufmerksam machen.

Erste Hilfe

wenn nötig: Notarzt holen: 09 19 222 und diese Betriebsanweisung vorzeigen

Nach Einatmen: Frischluft zuführen, Atemwege freihalten, ggf .Atemspende.

Nach Verschlucken: Wiederholt reichlich Wasser mit A-Kohle-Zusatz trinken lassen. Kein Erbrechen! Arzt hinzuziehen!

Als Laxans Na_2SO_4 (1 Eßlöffel auf 1 Glas Wasser) verabreichen.

Nach Hautkontakt: Sofort mit viel Wasser abwaschen.

Nach Kleidungskontakt: Kleidung entfernen und Haut wie oben behandeln.

Nach Augenkontakt: Mehrere Minuten bei geöffnetem Lidspalt unter fließendem Wasser spülen. Augenarzt hinzuziehen!

Bei Verbrennungen: Kleidung im Bereich der Verbrennung, soweit möglich, entfernen. Festklebende Teile umschneiden. Kaltwassertherapie wirkt noch bis 20 Minuten nach Hitzeeinwirkung. Brandwunden bis zum Eintreffen des Arztes mit sterilem Verbandmaterial abdecken.

Ersthelfer: siehe örtlicher Aushang

Sachgerechte Entsorgung

In den Sammelbehälter A2 (organische Verbindungen, halogenfrei, wasserarm) geben.

Gefährliche Reaktionen

allgemeines: bildet mit Luft oder Sauerstoff ein explosionsfähiges Gemisch; ist mit Wasserdampf flüchtig

explosive Reaktion mit Diboranen, Natriumperoxid, Oxidationsmitteln, Ozon, Perchlorylfluorid, Permangansäure, Peroxydischwefelsäure, Peroxymonoschwefelsäure, Salpetersäure, Silberperchlorat (der Komplex reagiert bei Stoß!) und Uranhexafluorid

heftige Reaktion und Entzündung mit Bromtrifluorid/Brompentafluorid, Chromtrioxid, Difluordioxid, Fluor, Iodpentafluorid und Nitrylperchlorat

heftige Reaktion unter starker Wärmeentwicklung mit Chlor und Chlorkohlenstoffen in Gegenwart von Leichtmetallen insbesondere Aluminium

Ungeeignete Werkstoffe: Gummi wird gelöst; Kunststoffe prüfen

Angaben zur Toxikologie

MAK:
Gefahr der Hautresorption,
A1: eindeutig als krebserzeugend ausgewiesener Stoff, der beim Menschen erfahrungsgemäß bösartige Geschwülste zu verursachen vermag.
Erbgutverändernd 3: Stoff, für den eine Schädigung des genetischen Materials der Keimzellen beim Menschen oder im Tierversuch nachgewiesen wurde.

TRK: 1 ml/m3 oder 3.2 mg/m3

TRGS 905:
Krebserzeugend, Kategorie 1: Stoff, der beim Menschen bekanntermaßen krebserzeugend wirkt.
Mutagen, Kategorie 2: Stoff, der als erbgutverändernd für den Menschen angesehen werden sollte.

Akute Toxizität:
LD50 (oral, Ratte): 930 mg/kg
LC50 (inhalativ, Ratte): 10000 ppm/7h
LDLO (oral, Mensch): 50 mg/kg

Wirkungscharakter und Toxizität:

Akute Wirkungen:

Nach Einatmen: Höhere Dampfkonzentrationen führen zu einer starken Depression des Zentralnervensystems mit anfänglicher Euphorie und Erregung, gefolgt von Kopfschmerz, Schwindel unregelmäßiger Sprache und auch Narkose. Konzentrationen um ein Volumenprozent wirken in kurzer Zeit tödlich. Schäden sind rebersibel (Frischluft!)
Nach Haut-/Augenkontakt: Flüssigkeit wirkt entfettend, reizt Haut und Schleimhäute und ist hautresorptiv.
Nach Verschlucken: Übelkeit und Erbrechen; dabei Aspirationsgefahr. Magenschmerzen und ZNS-Depression.
Nach Resorption: Kopfschmerz, Schwindel, Herzrythmusstörungen, Blutdruckabfall, Atemnot, Erregung, Krämpfe, Narkose, Herzkreislaufversagen, Atemlähmung und Tod.

Chronische Wirkungen:
Lange symptomfreie Latenzzeit

Die Einwirkung auch geringer Mengen führt zu Schädigung der Blutbildungsorgane und Bildung von Krebsgewebe. Die Folgen sind Anämie, Makrocytose, Leukopenie, Thrombocytopenie und Hämolyse. Äußere Symptome: Blässe, vielfältige Blutungsneigung, Gewichtsverlust, Unruhe, Erregbarkeit und Nervosität.

Giftnotruf

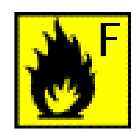
Physikalische Daten

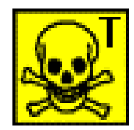
Molare Masse:	78.11,
Schmelzp.:	5,5 °C,
Siedep.:	80 °C,
d (20 °C):	0.879 g/cm3,
drel(Dampf):	2,7,
Dampfdruck:	100 hPa (mbar)/20 °C,
Dampfdruck:	350 hPa (mbar)/50 °C,
Flammpunkt:	-11 °C,
Zündtemp.:	555 °C,
Explosionsgrenzen von Luftgemischen:	1.2 - 8.0 Vol-%,
Löslichkeit (20 °C):	in Wasser: 0.7 g/l

Quellen

GefStoffV, Stoffliste (Bundesanzeiger), Benzol, B, 6/96
MAK-Liste 1996, Benzol
Sicherheitsdatenblatt, Merck, Benzol, 2/96
TRGS 900, Benzol, 11/96
TRGS 903, Benzol, 8/95
TRGS 905, Benzol, 5/96
Kühn-Birett, B012, 12/96
Roth-Weller, II B6, 12/90
Roth-Weller, III, Benzol, 4/96
Roth-Daunderer, B10, 6/96
BG Chemie, M025, 4/87

Universität Würzburg
Institut für Organische Chemie/Org.-chem. Praktika
UW - C 015
02/95





Benzol [71-43-2]

C_6H_6. Wasserunlösliche, farblose, charakteristisch riechende Flüssigkeit.

Gefahren für Mensch und Umwelt

Leichtentzündlich. Gefährliche Reaktionen mit starken Oxidationsmitteln oder mit Leichtmetallen in Gegenwart von Chlorkohlenwasserstoffen.

Giftig beim Einatmen, Verschlucken und bei Berührung mit der Haut.
Gefahr ernster Gesundheitsschäden bei längerer Exposition.
Benzol zeigt bei akuter oder chronischer Aufnahme unterschiedliche Wirkungen: Höhere Dampfkonzentrationen führen zu einer starken Depression des zentralen Nervensystems, zunächst treten jedoch Euphorie und Erregung auf. Danach folgen je nach Konzentration und Einwirkungszeit Kopfschmerzen, Schwindel, unregelmäßiges Sprechen und auch Bewusstlosigkeit. Höhere Konzentrationen sind nach kurzer Zeit tödlich. Bei rechtzeitiger Frischluftzufuhr bleiben keine Schäden zurück.
Flüssiges Benzol reizt die Haut und Schleimhäute und wirkt entfettend auf die Haut. Benzol wird leicht
durch die Haut aufgenommen! Bei Verschlucken folgen Magenschmerzen und bei verzögerter Entfernung auch Störungen des zentralen Nervensystems.
Die chronische Einwirkung führt nach langer, symptomfreier Latenzzeit zu Schädigungen der Blutbildungsorgane und Bildung von Krebsgewebe.
Stark wassergefährdender Stoff (WGK 3).

Schutzmaßnahmen und Verhaltensregeln

Im Abzug arbeiten! Exposition vermeiden. Von Zündquellen fernhalten.
Wenn möglich, Ersatzstoffe verwenden.

Schutzhandschuhe aus Latex und Neopren sind nicht gegen Benzol beständig (nur als sehr kurzzeitiger Spritzschutz verwendbar).

Verhalten im Gefahrfall (Unfalltelefon: 112)

Kleine Spritzer im Abzug verdampfen lassen, größere Mengen mit Absorptionsmaterial (Rench-Rapid) aufnehmen und entsorgen. Dämpfe nicht einatmen. Atemschutz: Kombinationsfilter ABEK. Brände mit CO2-Löscher bekämpfen!

Erste Hilfe

Nach Hautkontakt: Mit viel Wasser und Seife abwaschen.
Nach Augenkontakt: Mit Wasser mindestens 15 Minuten bei geöffnetem Lidspalt ausspülen. Augenarzt!
Nach Einatmen: Frischluft. Arzt!
Nach Verschlucken: Paraffinöl verabreichen. Erbrechen vermeiden. Arzt!
Nach Kleidungskontakt: Kontaminierte Kleidung sofort ausziehen.
Ersthelfer: siehe gesonderten Anschlag

Sachgerechte Entsorgung

Als Sondermüll (halogenfreie Lösungsmittel) entsorgen